



ViRobot Internet Security 2011

Guía del Usuario



Contenido

1. ViRobot Internet Security 2011	7
1.1 Información general	7
1.2 Requerimientos del Sistema	7
2. Características Principales	9
2.1 Centro de Seguridad	9
2.2 Análisis Rápido	11
2.3 Análisis Personalizado	13
2.4 Protección del Sistema	15
2.5 Configuración	37
2.51 Opciones de Análisis	37
2.52 Protección de Red	54
2.53 Protección de Datos	58
2.54 Mantenimiento	59
2.55 Otras Opciones	61
2.6 Actualización	69
2.7 Visor de Eventos	70
2.8 Cuarentena	72



Capítulo 1

ViRobot Internet Security 2011

Introducción

1. ViRobot Internet Security 2011

1.1 Información General

ViRobot Internet Security 2011 es un programa de seguridad para PC, desarrollado por Hauri Inc. Este programa provee funciones tales como análisis/reparación de virus informáticos, seguridad de red (Firewall, Anti-Phishing, Bloqueo de Sitios Web), Análisis de vulnerabilidades, Borrado permanente de archivos, Administración del Sistema, etc.

Para utilizar correcta y efectivamente ViRobot Internet Security 2011, por favor consulte los contenidos de esta Guía de Usuario.

1.2 Requerimientos del Sistema

Los requerimientos mínimos de Hardware/Software para la correcta ejecución de ViRobot Internet Security 2011 son los siguientes.

CPU	Pentium 3 500Mhz o superior
Memoria	512MB de memoria libre o superior
HDD	500MB de espacio libre o superior
OS	Windows 2000 Pro Windows XP Profesional (32bits, 64bits) Windows Vista (32bits, 64bits) Windows 7 (32bits, 64bits)



Capítulo 2

ViRobot Internet Security 2011

Características Principales

2. Características Personales

2.1 Centro de Seguridad



[Fig. 2.1] Interface del Centro de Seguridad

- El Centro de Seguridad consiste en un menú básico que es capaz de ejecutar funciones clave de ViRobot tales como Análisis Rápido, Análisis personalizado, y la protección del Sistema. También provee el menú que es capaz de ejecutar funciones adicionales tales como las Opciones, Visor de eventos, y la Cuarentena.
- Las Opciones de Seguridad son divididas en 3 niveles como se muestra en la siguiente gráfica.

Nivel \ Opciones de Seguridad	Opciones de Seguridad		
	Seguro	Moderado	Critico
Monitoreo en Tiempo Real	O	O	X
Firewall	O	X	X

➡ Opciones del Centro de Seguridad

① Análisis Rápido

- Analiza las carpetas predefinidos por el usuario.

② Análisis Personalizado

- Mediante la aplicación de configuraciones y áreas críticas definidas por el usuario, se realiza un análisis a detalle.

③ Protección del Sistema

- Se puede configurar la Seguridad de Red, Optimización del Sistema, Vulnerabilidades de Seguridad, Protección de Datos, y funciones adicionales. Para Opciones detalladas de cada opción, lea el "Capítulo 2.4 Protección del Sistema"

④ Inicio

- Esta opciones te regresa al Menú Principal da clic en el en cualquier otra ventana.

⑤ Opciones

- Funciones de Seguridad de ViRobot, tales como Opciones de Análisis, Protección de Datos, Seguridad de Internet, Cuarentena, Optimización de Sistema y Análisis de Vulnerabilidades. Si se habilita la opción de Activación de Contraseña para Configuración (ViRobot>Otras Opciones>Opciones Avanzadas) la configuración es bloqueada por el Administrador.

⑥ Ayuda

- Muestra la Información de Instalación de VRIS, Información de Soporte, Pagina Web, y la Ayuda.

⑦ Opciones de Monitoreo en Tiempo Real (Iniciar/Detener)

- Se puede configurar el monitoreo en tiempo real. Al detenerse el monitoreo en tiempo real se genera la ventana de notificación del estado del monitoreo en tiempo real y se modifica el estado de configuración de seguridad.
- En un estado peligroso de la configuración de seguridad aparece la configuración recomendada. El usuario puede fortalecer fácilmente la seguridad en el estado de configuración de seguridad alta con un solo clic a través de la función de configuración recomendada.



Referencia

La función de configuración recomendada, además de modificar el estado de monitoreo en tiempo real, reinicializa toda la configuración de VRIS a su configuración predeterminada.

⑧ Visor de Eventos

- El Visor de eventos nos muestra los registros de detección de malware, programas maliciosos, registros del sistema y errores.

⑨ Actualización

- Descargara cualquier actualización al nuevo motor y cualquier cambio en las funciones de ViRobot Internet Security. Entre las funciones de actualización se encuentra la actualización automática y la actualización programada. Para los contenidos detallados sobre las funciones de actualización, lea el “Capítulo 2.6 Actualización”.

⑩ Easy Robot

- Ejecuta un Análisis Rápido y la Optimización del Sistema con un solo clic.
- Si algún malware es detectado durante la ejecución de Easy Robot, este actúa de acuerdo la configuración especificada en el Análisis Básico. La función de reparación de Easy Robot es la siguiente: Si la reparación es posible, se realiza la reparación o se borra el archivo de manera automática. Si la reparación no es posible, falla la reparación y no realiza ninguna acción sobre el archivo.

2.2 Análisis Rápido



[Fig. 2.2] Centro de Seguridad – Análisis Rápido

- El Análisis Rápido, solo escanea las rutas predefinidas y rutas críticas del disco duro.

➡ Ventana de Análisis

En la ventana de Análisis Rápido nos muestra la información actual del análisis de VRIS, la carpeta analizada, y los nombres de los archivos. El usuario puede visualizar los elementos procesados, así mismo puede pausar, iniciar o cerrar el Análisis Rápido. La opción de vista detallada provee la información detallada de los elementos y la información de las amenazas. El sistema puede ser apagado de acuerdo a la configuración realizada por el usuario, si al finalizar el análisis no se detecta ninguna amenaza.

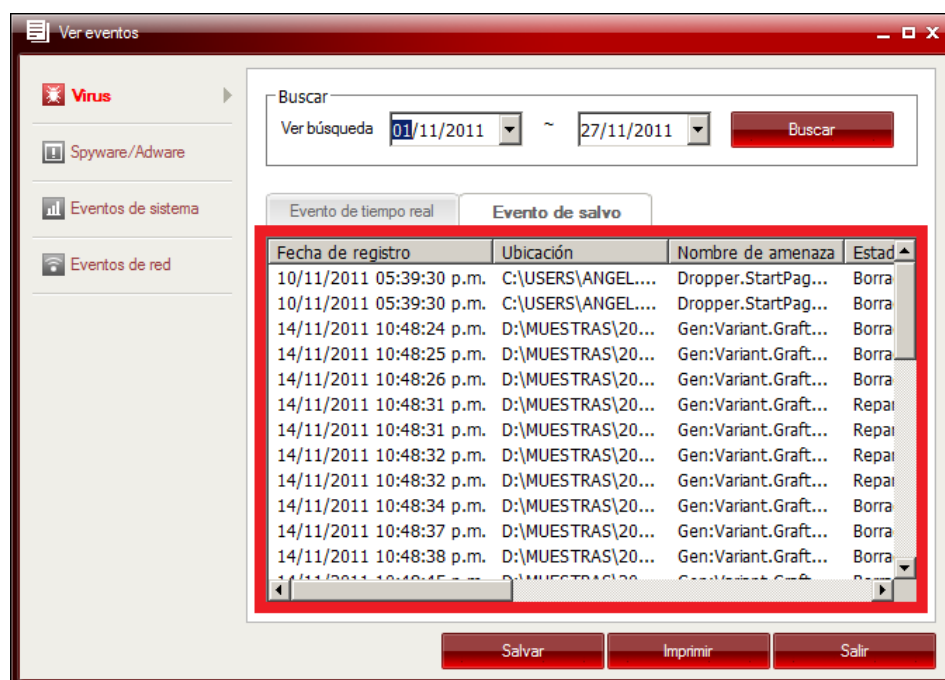


[Fig. 2.3] Ventana de Análisis Rápido

Cuando se está ejecutando un análisis, el icono de VRIS () cambia y muestra un círculo color verde. También cuando el análisis esta en progreso, el usuario puede pausar o continuar con el análisis. La ventana del análisis rápido básicamente muestra descripciones breves. Para una vista detallada de la información cuando algún malware es detectado, damos clic en Vista detallada y la ventana inferior del análisis se expenderá hacia abajo.

En la pantalla de la vista detallada, se muestra en tiempo real la información del malware detectado. Si el malware puede ser reparado seleccionando el elemento.

El historial de reparación de malware puede ser visto en la pestaña “Eventos de salvo” en la función de Visor de Eventos de VRIS.



[Fig. 2.4] Registro Análisis Rápido



Referencia

- ✖ Como el Análisis Rápido solo verifica carpetas específicas, no todas las amenazas son detectadas. Si deseas realizar un análisis completo o a diferentes carpetas, debemos seleccionar Análisis Personalizado.

2.3 Análisis Personalizado



[Fig. 2.5] Centro de Seguridad – Análisis Personalizado

Como el explorador de Windows, analiza el malware seleccionando la carpeta o unidad deseada. Al seleccionar las carpetas y unidades de análisis y haciendo clic en iniciar análisis, el análisis se ejecuta y detecta los archivos maliciosos en las carpetas seleccionadas. Por el momento, analiza el malware que con los valores de configuración de análisis básico.

El usuario puede configurar la cuarentena y el Análisis Personalizado en la ventana de Análisis Personalizado. Para la configuración detallada de cuarentena y Análisis Personalizado, vea Configuración de “Capítulo 2.2 Análisis Básico” y “Capítulo 2.8 Cuarentena”.



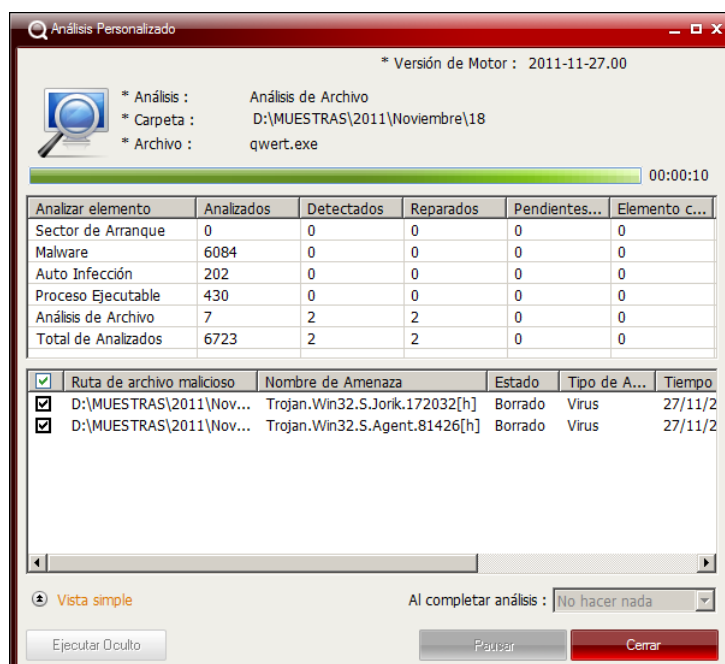
[Fig. 2.6] Selección de Carpeta en Análisis Personalizado

➡ Ventana de Análisis

Especificar los objetivos del Análisis personalizado seleccionando carpetas. Al seleccionar las carpetas para análisis, explora las carpetas, subcarpetas y archivos. Al terminar la selección para análisis, ejecutar el análisis haciendo clic en el botón de inicio del análisis.

En el Análisis Personalizado, el tipo de análisis se muestra en la parte superior izquierda de la ventana. Cuando se selecciona la opción en Análisis Básico, se selecciona sector de arranque, programas no deseados, auto infección, análisis de procesos y análisis de archivos, se analizarán en el orden seleccionado.

Una vez finalizado el Análisis Personalizado, reparar el malware detectado haciendo clic en el botón de reparación en la ventana de la vista de detalle.



[Fig. 2.7] Selección de Reparación en Análisis Personalizado



[Fig. 2.8] Reparación después de Análisis Personalizado

2.4 Protección de Sistema



[Fig. 2.9] Centro de Seguridad – Protección de Sistema



[Fig. 2.10] Protección de Sistema – Protección de Red

- La Protección del Sistema ejecuta básicamente la protección de red, Optimización del Sistema, Vulnerabilidades de Seguridad, Protección de Datos y Otras Opciones. Si el usuario selecciona la Protección del Sistema, aparece la ventana de Protección de Red y las funciones siguientes.

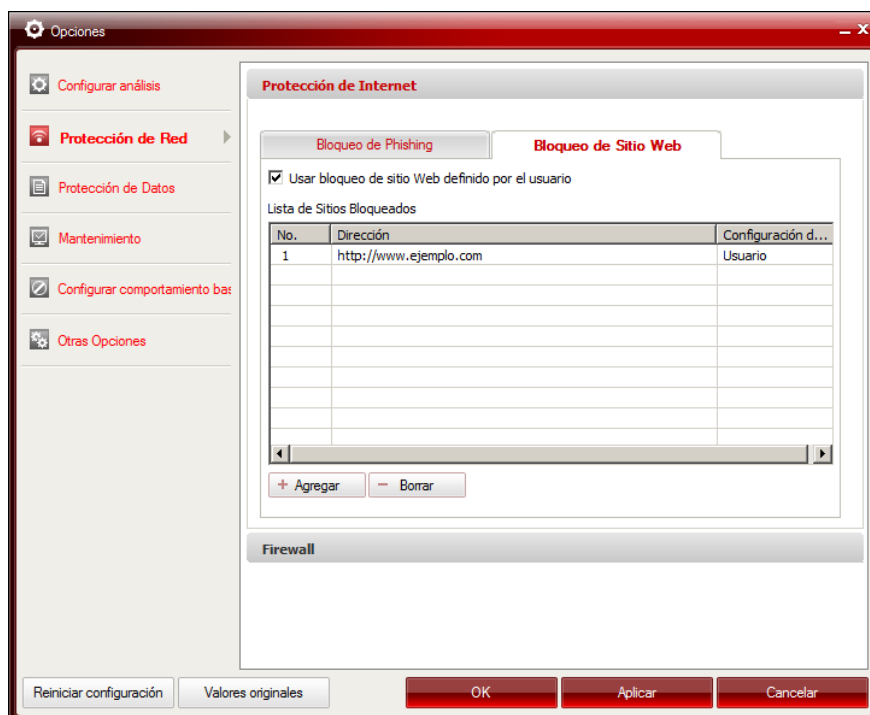
① Protección de Red

➡ Anti-Phishing



[Fig. 2.11] Anti-Phishing

- Anti-Phishing: Es la función para prevenir fugas de información privada y financiera del usuario. En el caso de acceso a sitios de phishing identificados, VRIS bloquea el acceso a internet y muestra una ventana de bloqueo al usuario.
- Bloqueo de Sitios Web: En el caso de acceso a los Sitios definidos por el usuario en las reglas de filtrado, VRIS bloquea el acceso y muestra una ventana de bloqueo al usuario. Básicamente, El filtrado Web tiene una regla que permite el acceso, y el usuario deberá escribir las direcciones de Sitios Web que desea bloquear.



[Fig. 2.12] Listado de Sitios Bloqueados

- Los usuarios de VRIS deberán ingresar direcciones de acceso a internet. Para dominios bloqueados, se bloquea el acceso y aparece la página de error del navegador web. Se admite la función de bloqueo de sitios web para los navegadores, tales como Firefox, Internet Explorer y Google Chrome que estén instalados en el Sistema Operativo Windows.

➡ Firewall



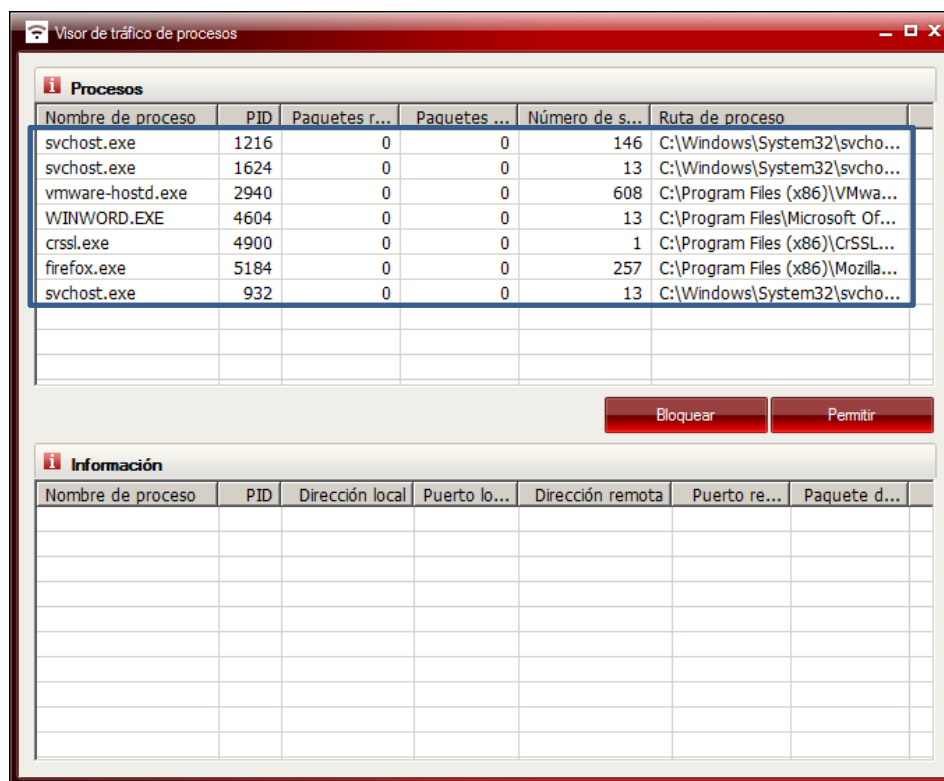
[Fig. 2.13] Firewall

- Servicio de Protección de Red: Muestra el estado de los bloqueos de las intrusiones de red y el estatus de ejecución del servicio del Firewall. El usuario de VRIS puede iniciar o detener el servicio de Protección de Red. Si el estatus es modificado, se informa en la pantalla principal de VRIS (Centro de Seguridad), y se muestra una ventana de notificación (Fig. 2.13).
- Monitoreo de red: Muestra con graficas en tiempo real la utilización de la red de VRIS. Para la configuración de las reglas de Firewall, vea "Capítulo 2.52 Configuración – Firewall".



[Fig. 2.14] Monitoreo de Red

- Vista Detallada: Al ejecutar el Visor de Trafico de Procesos, muestra la información de uso de red de los procesos. Para los procesos que causan tráfico, el usuario puede automáticamente generar una regla de bloqueo de procesos en el Firewall Personal, como se muestra en la siguiente imagen.



[Fig. 2.15] Visor de Trafico de Procesos



② Optimizar Rendimiento



➡ Mantenimiento



[Fig. 2.18] Mantenimiento

- **Buscar:** Esta opción busca información privada del usuario, archivos utilizados por aplicaciones. Los elementos que se buscan son los siguientes.
 - ✓ **Uso de Navegadores de Internet**
 - Cookies
 - Autocompletado
 - Historial de Navegación
 - Direcciones Abiertas
 - Archivos Temporales de Internet
 - ✓ **Lista de Archivos utilizados recientemente**
 - Microsoft Paint
 - WordPad
 - Microsoft Office Word
 - Mis Documentos Recientes
 - Windows Media Player
 - ✓ **Lista de Ejecución**
 - Ejecutar
 - Búsqueda de archivos
 - Búsqueda de Computadoras
 - Escritorio Remoto
- **Gestionar:** Se eliminan los elementos seleccionados por el usuario.

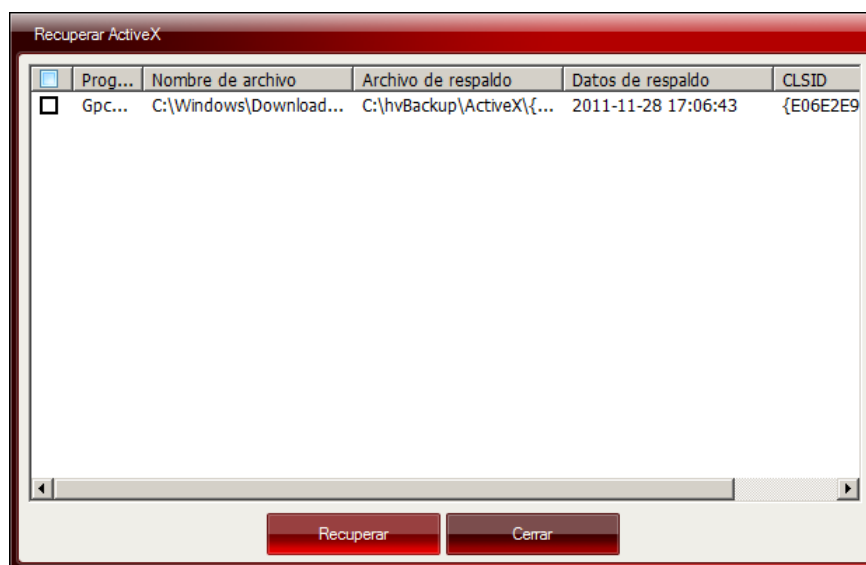
➡ Control ActiveX



[Fig. 2.19] Control ActiveX

- La Función Control de ActiveX muestra los elementos ActiveX instalados en el sistema, pueden ser removidos o recuperados por el usuario.

➤ Recuperar: El usuario puede recuperar los ActiveX eliminados.



[Fig. 2.20] Recuperación de ActiveX

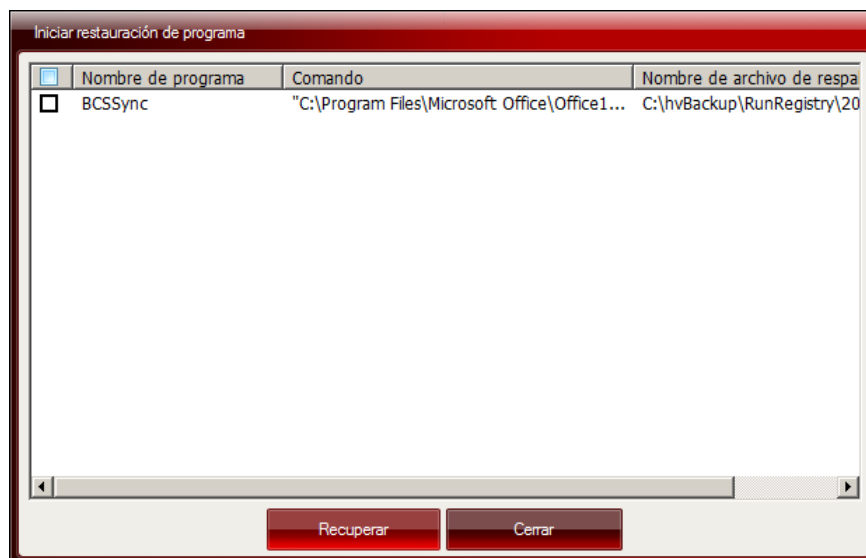
➤ Remove: Se muestran los ActiveX instalados que han sido eliminados. Pueden ser restaurados utilizando la función de recuperación, los ActiveX activos no pueden ser removidos.

➡ Control de Programas de Inicio



[Fig. 2.21] Control de Programas de Inicio

- Esta opción controla los elementos establecidos en el Inicio de Windows.
 - Remove: El usuario selecciona los elementos innecesarios de la lista. Los elementos eliminados pueden ser recuperados a través de la función de recuperación.
 - Recuperar: Esta opción recupera los elementos eliminados por el usuario a través de VRIS.



[Fig. 2.22] Restauración de Programas de Inicio

③ Análisis de Seguridad



[Fig. 2.23] Análisis de Seguridad

- Al analizar las vulnerabilidades de seguridad en la computadora del usuario y protegiendo el sistema de amenazas de atacantes, se proporciona al usuario un ambiente de red seguro.

➡ Actualizaciones de Windows

- Analizar parches de seguridad: al analizar los últimos parches de seguridad instalados en el sistema operativo Windows, se muestran las actualizaciones, nivel, prioridad e instalación. Si selecciona un elemento no instalado, se le ayudará a realizar la conexión al sitio de actualización de Microsoft.



[Fig. 2.24] Análisis de parches de Windows

➡ Análisis de Cuentas de Usuario



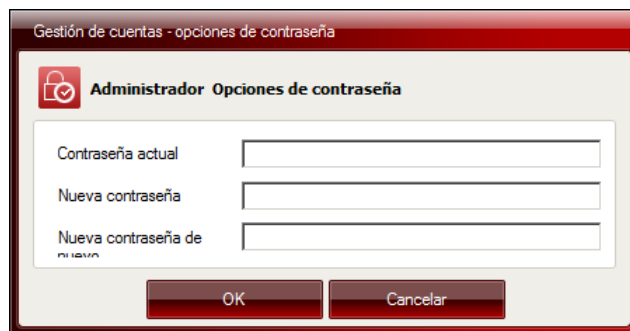
[Fig. 2.25] Análisis de Cuentas de Usuario

- Analizar cuentas: Muestra la información de la cuenta actual. Si la cuenta de Invitado o cualquier cuenta no tiene contraseña, puede ser blanco de algún ataque de virus.



[Fig. 2.26] Ajustes de cuentas de usuario sin contraseña

- Cambio de contraseña: Después de realizar un análisis de las cuentas de usuario, especifica una contraseña a la cuenta. Para las cuentas sin contraseña no es necesario introducir la contraseña actual. Incluso para las cuentas existentes, si se introduce la contraseña actual, el usuario puede establecer una nueva contraseña.



[Fig. 2.27] Cambio de contraseña



[Fig. 2.28] Análisis de Cuentas de Usuario después de cambiar contraseña

- Verificación de cuenta: La configuración de la cuenta puede administrarse en el Panel de Control de Windows. Las cuentas de usuario locales pueden ser administradas en el opción Cuentas de Usuario en el Panel de Control de Windows.

➡ **Análisis de Carpetas Compartidas**



[Fig. 2.29] Análisis de Carpetas Compartidas

- **Remover recurso:** Se muestra la lista actual de carpetas compartidas. Como algunos virus pueden introducirse a través de las carpetas compartidas, se necesita verificar si el usuario a olvidado cancelar las carpetas compartidas después de su uso o si la compartición de alguna carpeta ha sido establecida por virus, esta función ayuda a administrar las carpetas compartidas.

④ **Protección de Datos**



[Fig. 2.30] Protección de Datos

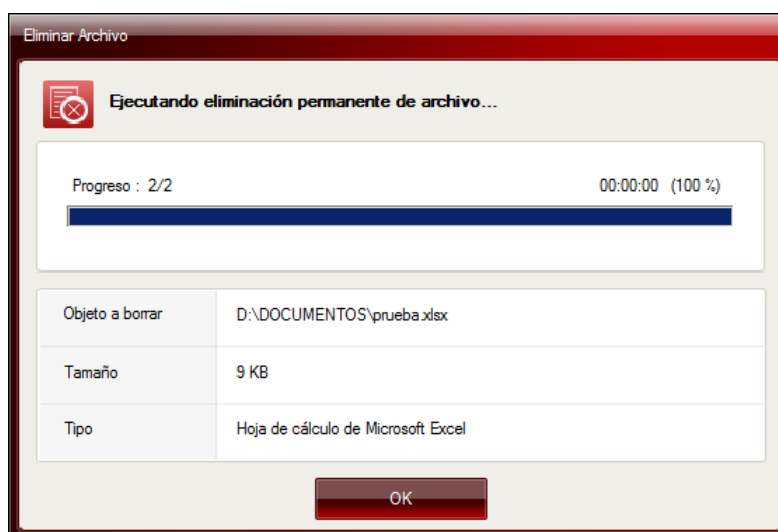
- Esta es la función para proteger la información confidencial del usuario, y provee la función de eliminado permanente de los archivos.

➡ Eliminar Archivo



[Fig. 2.31] Eliminar Archivo

- Añadir Archivo: Selecciona los archivos en la Unidad de Disco para su eliminación permanente. Después de seleccionar los archivos, estos son agregados a la ventana de eliminación permanente.
- Eliminar Archivo: Al aplicar la configuración "Borrado permanente de Archivos", los archivos seleccionados por el usuario son eliminados de manera permanente.



[Fig. 2.32] Ventana de avance de eliminación de Archivos



[Fig. 2.33] Eliminación de Archivos completado

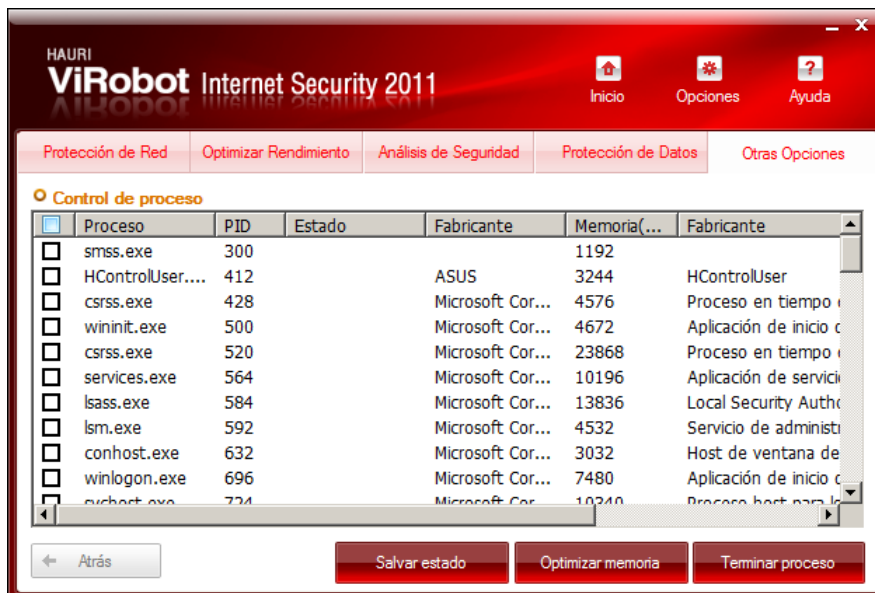
⑤ Otras Opciones



[Fig. 2.34] Otras Opciones

- Como Otras Opciones de VRIS tenemos, Control de Proceso, Opciones de Sistema y Control de Uso de PC.

➡ Control de Proceso



[Fig. 2.35] Control de Proceso

- En este función se muestra la información de los procesos activos del sistema y se provee la función de Administrador de tareas.
 - Salvar Estado: Se guarda el estatus actual del sistema.
 - Optimizar Memoria: Recupera la memoria de procesos sin uso, esta opción incrementa la memoria disponible.
 - Terminar Proceso: El procesos seleccionado por el usuario es terminado.

➡ Opciones de Sistema



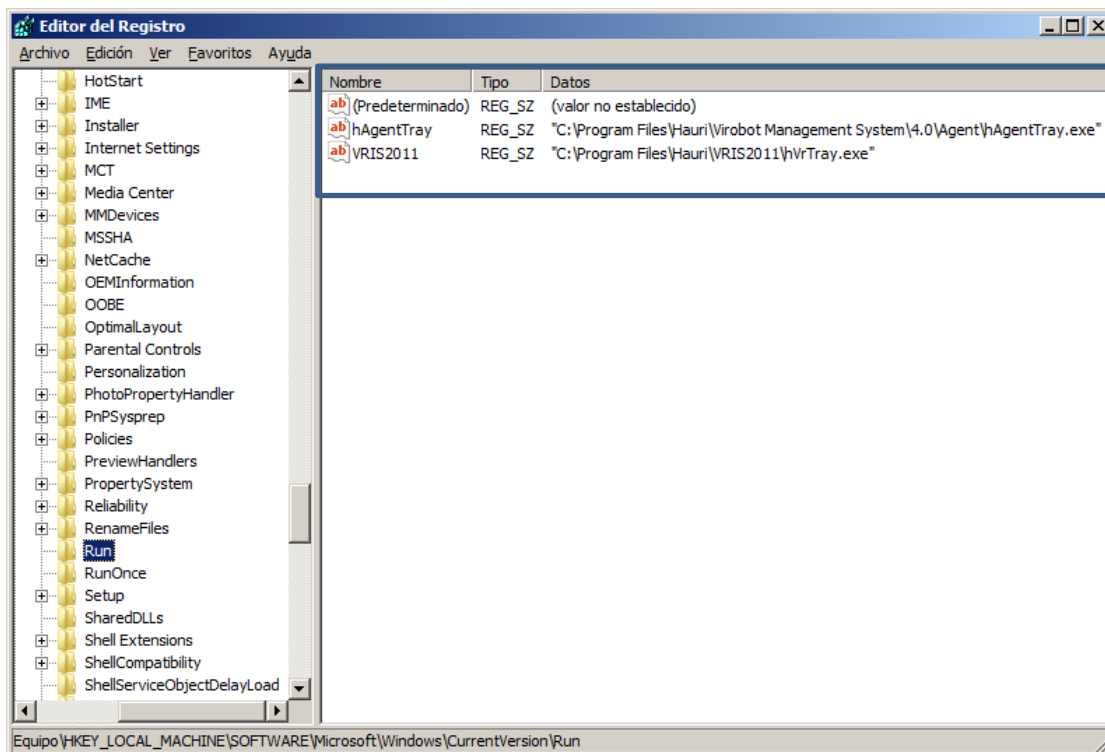
[Fig. 2.36] Opciones de Sistema

- En esta función se mejora la facilidad de uso, proporcionando la configuración de los programas de inicio, opciones de internet y configuración del menú de exploración de Windows. Se han desactivado los valores por defecto.

a) Opciones de Inicio/Salida de Windows

- Desactivar registro de inicio: Se Habilitan/Deshabilitan programas de inicio especificados en Windows. Al seleccionar la opción “Desactivar Menú EJECUTAR”, se deshabilita lo registrado en las llaves siguientes.

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce



[Fig. 2.37] Programas de Inicio en el Registro de Windows

- Borrar lista de documentos recientes al apagado (Windows XP o superior): Esta opción elimina los registros de documentos abiertos recientemente al apagar el sistema. Los archivos son eliminados después de reiniciar el sistema.
- Deshabilitar auto ejecución (Requiere reinicio): Deshabilita el autorun de Windows, el que reconoce automáticamente medios extraíbles. Esta opción aplica al reiniciar el equipo y solo para Windows XP.

b) Opciones de Navegador de internet

- **Página de Inicio:** El usuario puede seleccionar una dirección web como página de inicio del navegador de internet. Si ya existe una página de inicio se podrá visualizar en esta opción. Esta función solo es soportada para MS Internet Explorer.



[Fig. 2.38] Página de Inicio



Referencia

- ✖ Luego de configurar la página de inicio, si no se configuro correctamente aparecerá la página de error. Verifique la configuración de la página de inicio.

- **Ruta de descargas:** Es la función donde se selecciona la ruta donde serán guardados los archivos descargados por el usuario. Se mejora el manejo de las descargas del navegador web. Esta función solo es soportada para MS Internet Explorer.



[Fig. 2.39] Ruta de Descargas de MS Internet Explorer

- Deshabilitar reporte de errores de Internet: Esta opción deshabilita el reporte de errores cuando el proceso del navegador (iexplore.exe) es terminado de manera anormal. Esta opción se encuentra en Mi PC-Propiedades-Avanzadas-Reporte de Errores.



[Fig. 2.40] Deshabilitar reporte de errores de Internet



Referencia

- ✖ Se deshabilita la función de Reporte de Errores, excepto para BSOD (Pantalla azul), el reporte de errores para aplicaciones no es soportada.

c) Opciones de uso de Sistema y Explorador

- **Deshabilitar Panel de Control:** Esta opción restringe el uso del Panel de Control. Cuando el estatus es deshabilitado, se cambian los elementos del Panel de Control a modo oculto y bloquea la ejecución de estos elementos a través del menú ejecutar. Esta opción es habilitada hasta después de reiniciar el Explorador de Windows (explorer.exe), y la función esta activa como se muestra en la siguiente figura.



[Fig. 2.41] Deshabilitar Panel de Control

Lista de Funciones de Panel de Control		
Centro de accesibilidad	Reconocimiento de voz	Dispositivos de Juegos
Agregar/Quitar programas	Teléfono y modem	Mouse
Pantalla	Fecha y hora	Dispositivos de Sonido y Audio
Agregar nuevo hardware	Cuentas de usuario	Conexiones de Red
Opciones de Internet	Administración de discos	Puerta de enlace de red
Configuración Regional y de idioma	Resultado de Aplicación de políticas	Opciones de Energía
Puerto Infrarrojo	OBDC	

- **Deshabilitar administrador de tareas:** Se restringe el uso de las funciones que provee el administrador de tareas. Generalmente, el Administrador de tareas es ejecutado usando la combinación de teclas (Ctrl+Alt+Supr), (Shift+Ctrl+Esc), ejecutando el comando taskmgr en el menú ejecutar o desde botón derecho en la barra de tareas. Cuando esta opción esta activada, todas las opciones son deshabilitadas.



[Fig. 2.42] Deshabilitar Administrador de tareas

- **Deshabilitar ventana de comando:** Se restringe el uso de línea de comandos, que es la consola de aplicaciones provista por Windows.



[Fig. 2.43] Deshabilitar Ventana de Comando



Referencia

- ✖ Cuando la ventana de comando está restringida, la ejecución de comandos a través de batch esta deshabilitada. Cuando se vayan a ejecutar comandos vía batch, asegúrese de tener deshabilitada esta opción.

- Deshabilitar ventana ejecutar (requiere reiniciar explorer): Restringe la opción ejecutar de Windows. Si se aplica esta restricción, dicha opción se del Explorador de Windows (explorer.exe).



[Fig. 2.44] Deshabilitar Ventana Ejecutar

- Deshabilitar Explorador de Windows > Vista de Opciones de Carpeta: Esta opción restringe el menú "Opciones de Carpeta". Evitando el cambio de configuración de las carpetas.
- Deshabilitar Explorador de Windows > Opciones de archivos/carpetas ocultos: Esta opción restringe las opciones de archivos/carpetas ocultos en el Explorador de Windows. Los archivos o carpetas ocultos son mostrados como iconos con transparencia y son removidos de la vista de las ventanas.

➡ Control de Uso de PC

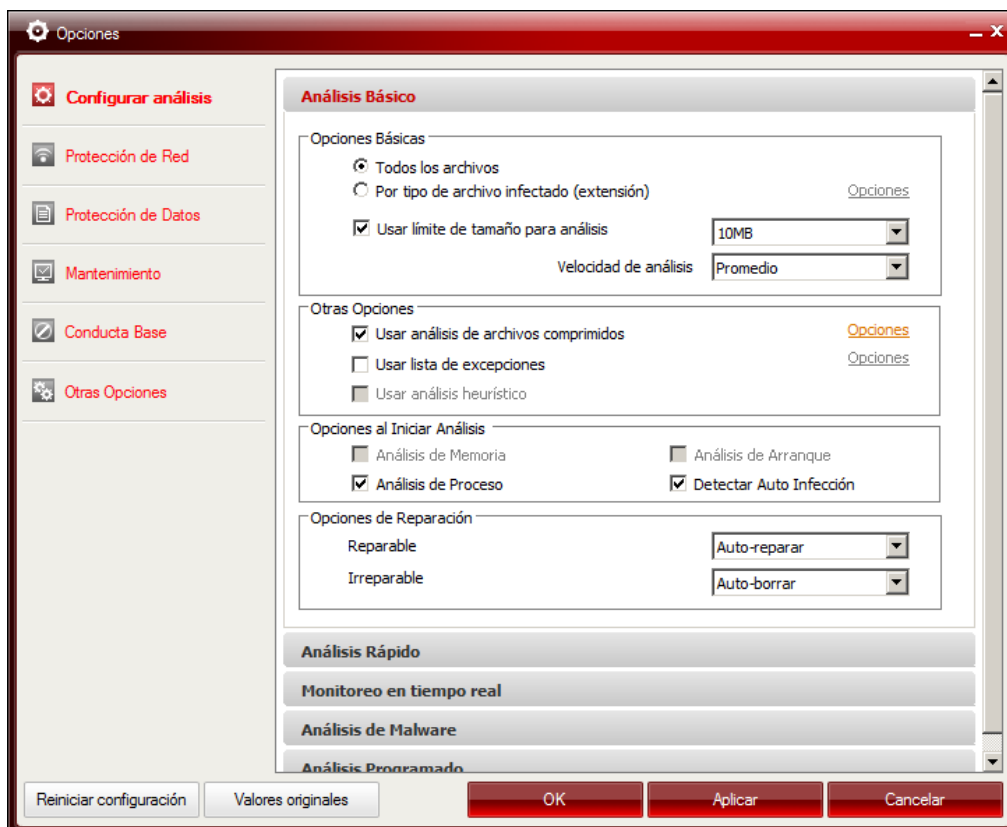


[Fig. 2.45] Control de Uso de PC

- Se puede bloquear el uso de la PC y de la red en la fecha y en el horario correspondiente configurando el cuadro de programación. El usuario puede configurar la hora del uso de PC a través del arrastre o click del mouse en el gráfico. Para desactivar el Control de Uso de PC, es necesario introducir la contraseña del Administrador.

2.5 Opciones

2.5.1 Configurar Análisis

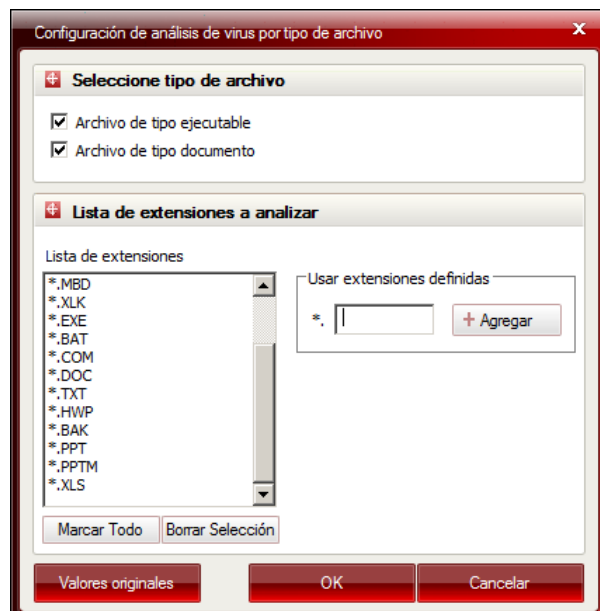


[Fig. 2.46] Opciones de Análisis Básico

① Análisis Básico

a) Opciones Básicas

3. Todos los archivos: Esta opción escanea todos los tipos de extensiones. Esta es la opción por defecto.
4. Por tipo de archivo infectado (extensión): El usuario selecciona directamente los elementos de infección. Los elementos disponibles son, archivos ejecutables, documentos y las extensiones definidas por el usuario.



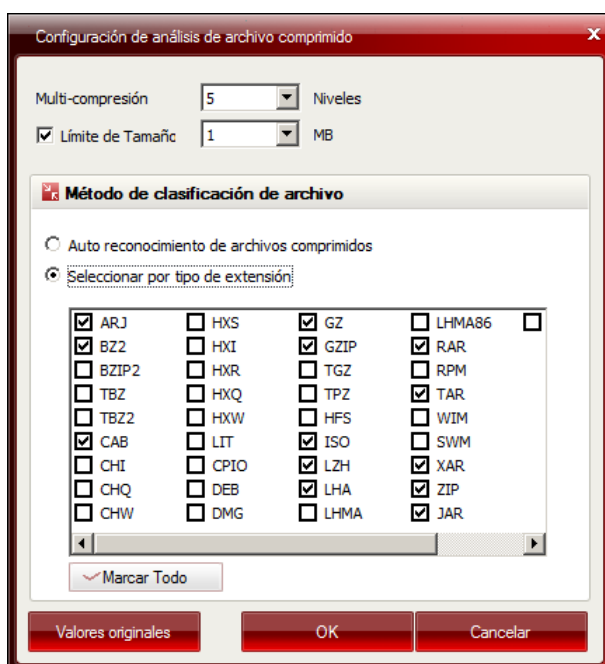
[Fig. 2.47] Opciones avanzadas de Análisis de virus por tipo de archivo

EXE	BAT	COM	DOC	TXT	HWP	BAK
PPTM	XLS	XLSX	PDF	HTM	MBD	XLK
PPT						

- Usar límite de tamaño para análisis: Esta opción restringe el tamaño máximo de los archivos a escanear. Para esta opción, el usuario puede seleccionar entre 1MB y 5GB, el valor por defecto es 1GB.
- Velocidad de Análisis: Opción para seleccionar la velocidad del análisis. El usuario puede seleccionar entre Mínimo, Promedio, Máximo, y la velocidad del análisis cambia según la configuración. El valor por defecto es Promedio (Recomendado).

b) Otras Opciones

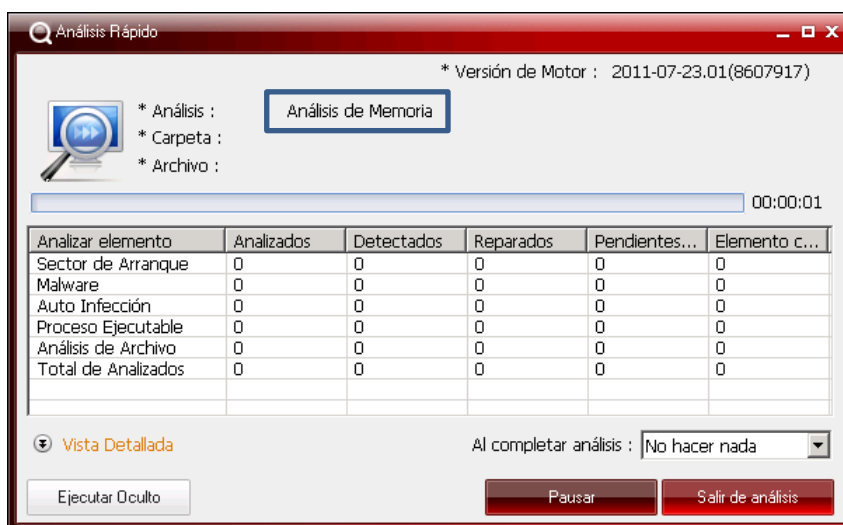
- Usar Análisis de Archivos comprimidos: Se selecciona el nivel, límite de tamaño, y tipos de archivos comprimidos para analizar. Para Multi-compresión, el usuario puede establecer desde el nivel 1 hasta el 5. El límite de tamaño de archivos comprimidos está establecido a 1, 3, 5 y 10MB, y el valor por defecto es 1MB. VRIS soporta el análisis de archivos comprimidos por extensión establecidos en la siguiente tabla. El valor por defecto detecta automáticamente los archivos comprimidos.



[Fig. 2.48] Opciones de Análisis de Archivos Comprimidos

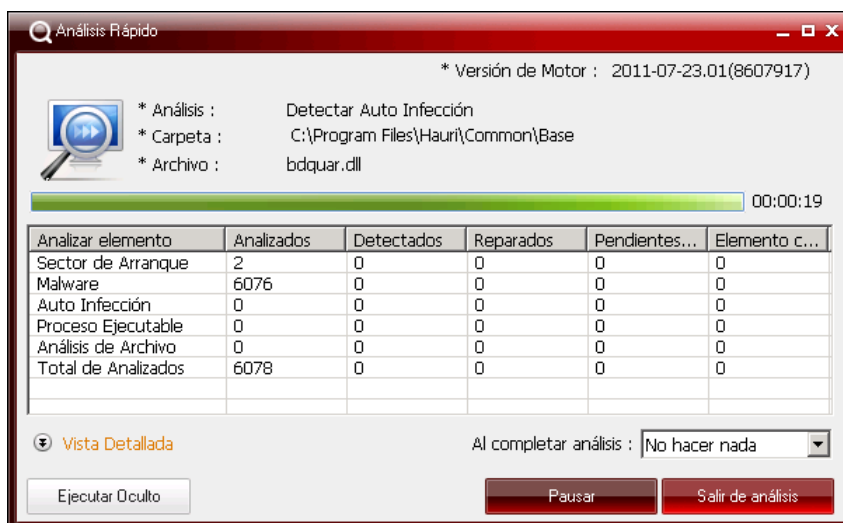
- Usar lista de excepciones: Se pueden realizar exclusiones al análisis especificando la carpeta, archivos y extensiones cuando se ejecute un análisis rápido, análisis programado, análisis personalizado o un análisis con el botón derecho del mouse. Se agregan carpetas y archivos a la exclusión, a través del Explorador de Windows. Cuando se agregan extensiones a la exclusión, se hace de manera manual. (No hay configuración por defecto para esta opción).
 - Usar Análisis Heurístico: Analizar y detectar todos los archivos sospechosos para no perder ningún archivo malicioso.
- c) Opciones al Iniciar Análisis: Se realiza un análisis de memoria, procesos, sector de arranque y auto-infección, antes de realizar un análisis de archivos, ya sea un análisis rápido, análisis programado y un análisis personalizado. El orden de Análisis es: Memoria > Malware > Auto-infección > Procesos > Archivos. (Por defecto está habilitado: Análisis de Memoria, Sector de Arranque, Procesos y Auto-Infección).

- ✓ **Análisis de Memoria:** Se analiza la memoria en el sistema donde está instalado VRIS.



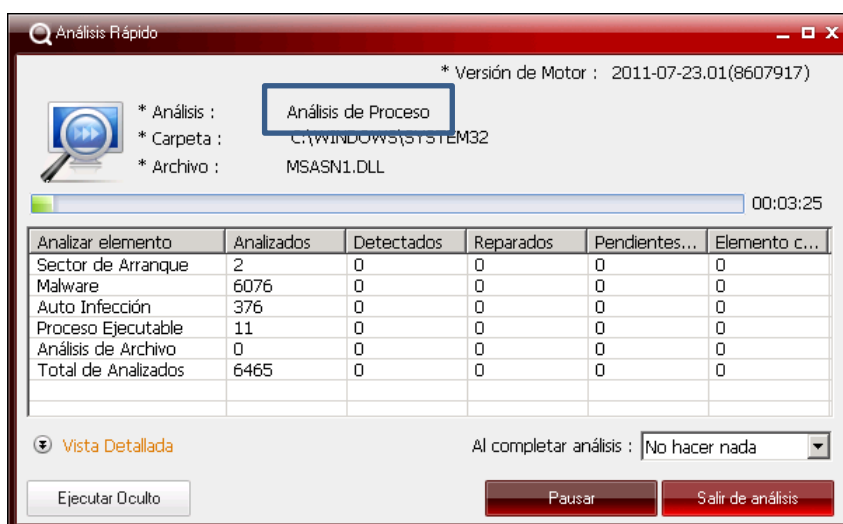
[Fig. 2.49] Análisis de Memoria

- ✓ **Análisis de Arranque:** Se analiza el sector de arranque existe en FDD y HDD. Análisis de arranque detecta infecciones de código malicioso cuando se ejecute un análisis rápido, análisis programado o análisis personalizado.
- ✓ **Detectar Auto-Infección:** Realiza un análisis de malware en las carpetas de instalación. Si la detección de Auto-Infección está habilitada, básicamente, protege de código malicioso los productos de Hauri, analizando la carpeta c:\Archivos de Programa\Hauri.



[Fig. 2.50] Detección de Auto Infección

- ✓ **Análisis de procesos:** Analiza los procesos activos en el sistema. Analiza los archivos ejecutables de los procesos de acuerdo a la lista de programas del sistema.



[Fig. 2.51] Análisis de procesos

d) Opciones de reparación

- **Reparable:** Si el código malicioso que es detectado se puede reparar, se actúa de acuerdo a la configuración, ya sea Ignorar, Auto-reparar o Auto-Borrar. (Valor por defecto: Reparar automáticamente).
- **Irreparable:** Si el código malicioso que es detectado no se puede reparar, se actúa de acuerdo a la configuración, ya sea Ignorar, Auto-reparar o Auto-Borrar. (Valor por defecto: Ignorar).

➡ Ignorar, si la reparación es posible

- ▼ Solo notifica la información de la detección, y el usuario repara manualmente después de seleccionar el código malicioso. Los usuarios con autorización pueden reparar los códigos maliciosos detectados seleccionándolos en la vista de Vista Detallada.

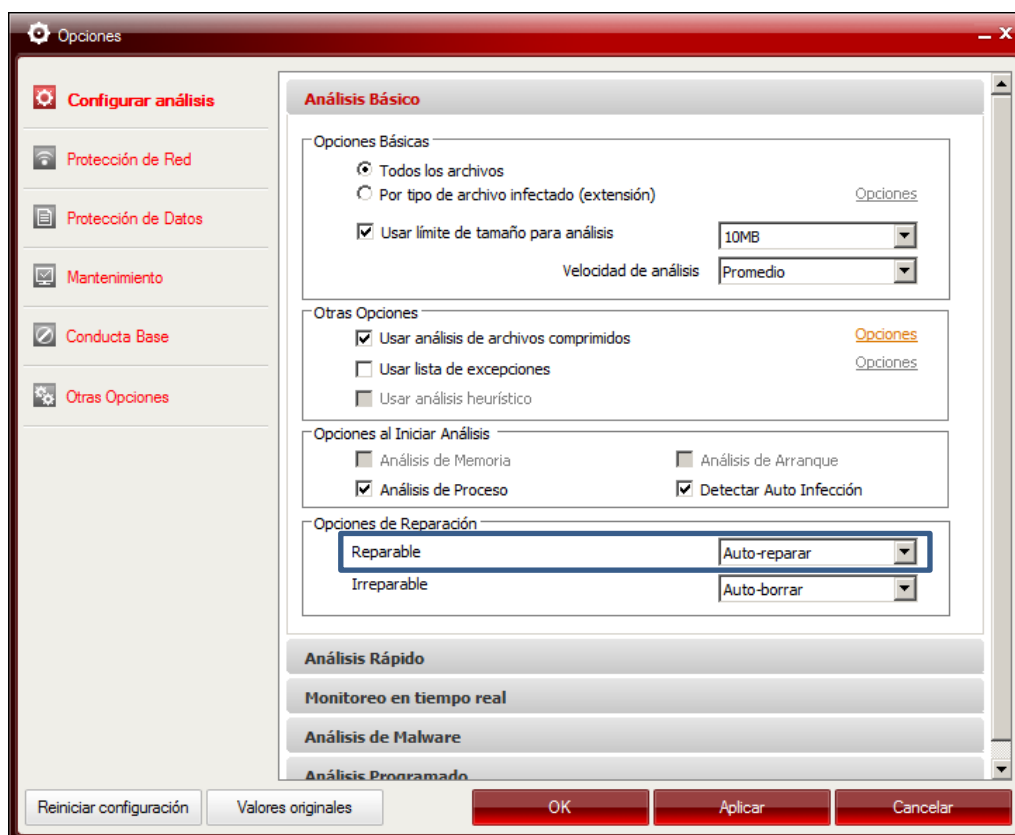


Referencia

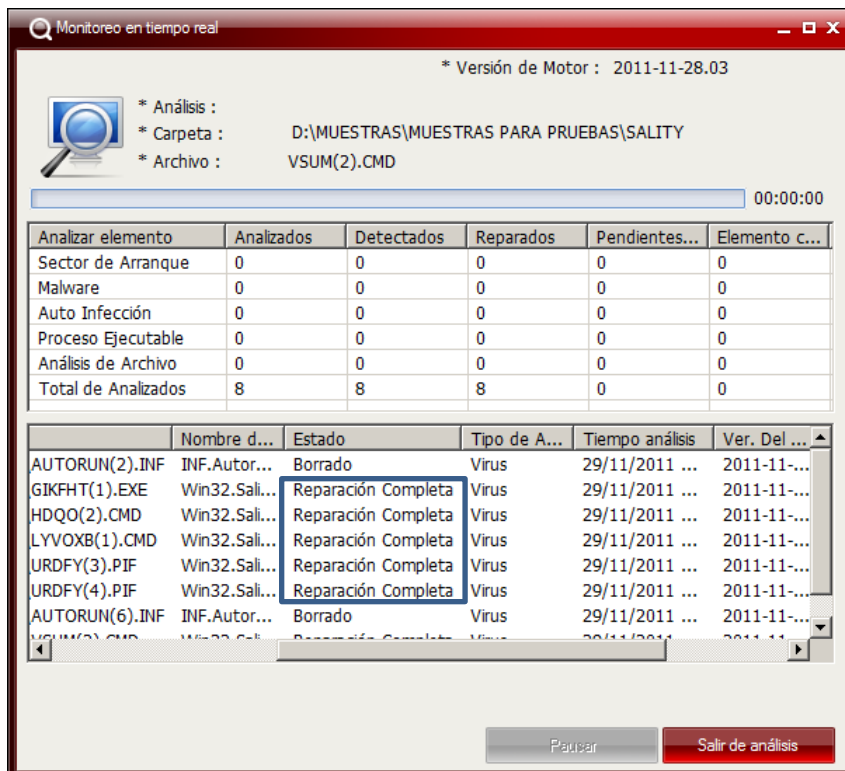
- ✖ Para "Ignorar", la función de reparación no se muestra en la vista simple. Para áreas inaccesibles del Sistema Operativo (Ej. Sectores de arranque, Unidades de CD), la reparación fallara debido a la autorización de acceso.

➡ Auto-reparar, si la reparación es posible

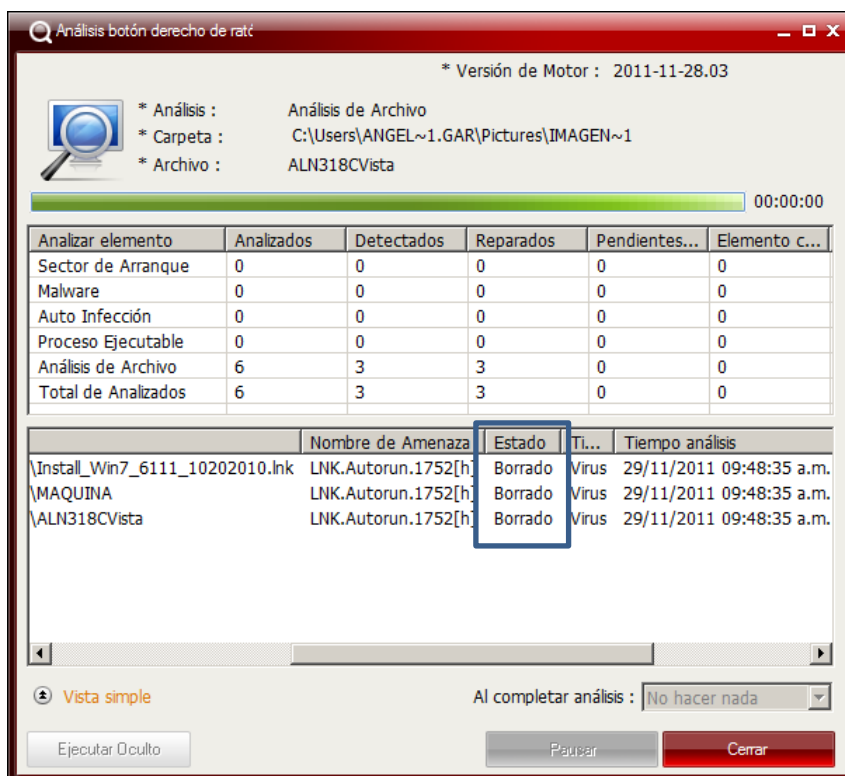
- ▼ Repara automáticamente los códigos maliciosos detectados. Si la reparación de código malicioso es posible, se muestra el estatus de reparación. Si la reparación es posible pero es un archivo, se muestra el tipo de reparación. Por ejemplo, si el tipo de amenaza es una macro de MS Word, el estatus muestra reparación no eliminación del archivo, ya que elimina solo el área de la macro.



[Fig. 2.52] Auto-reparar, si es posible



[Fig. 2.53] Auto-reparación de archivos



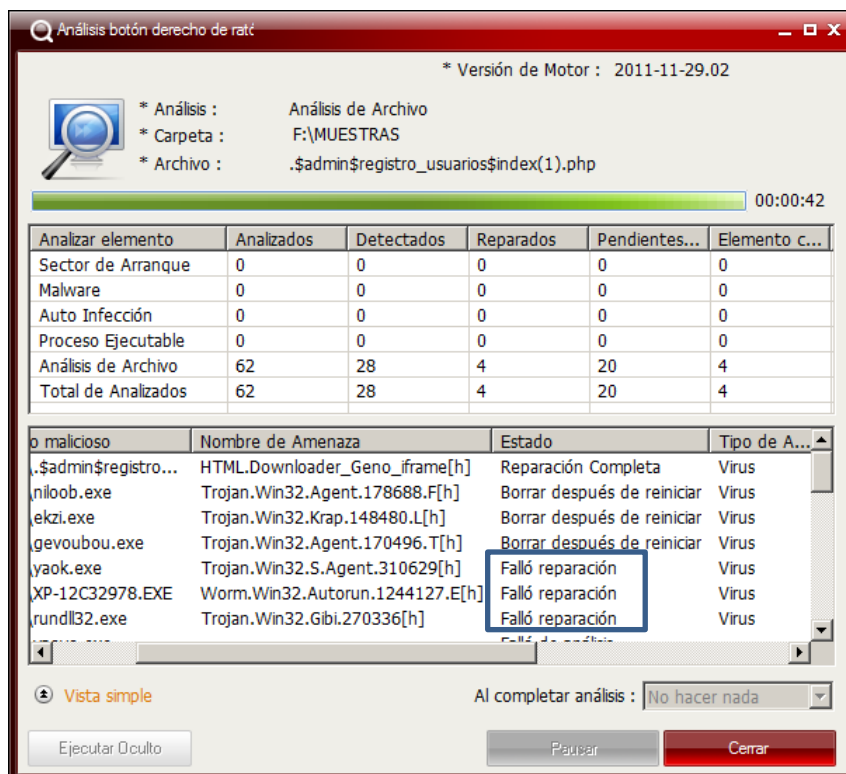
[Fig. 2.54] Auto-reparación de archivos

➡ Ignorar, si la reparación falla

- ▼ Esta opción solo notifica la detección de código malicioso, el usuario podrá eliminar el archivo manualmente al seleccionarlo. Los usuarios con autorización pueden reparar los códigos maliciosos detectados seleccionándolos en la vista de Vista Detallada.

➡ Auto-borrar, si la reparación falla

- ▼ Si la reparación del código malicioso falla, el archivo se eliminara automáticamente.



[Fig. 2.55] Auto-borrar, si la reparación falla

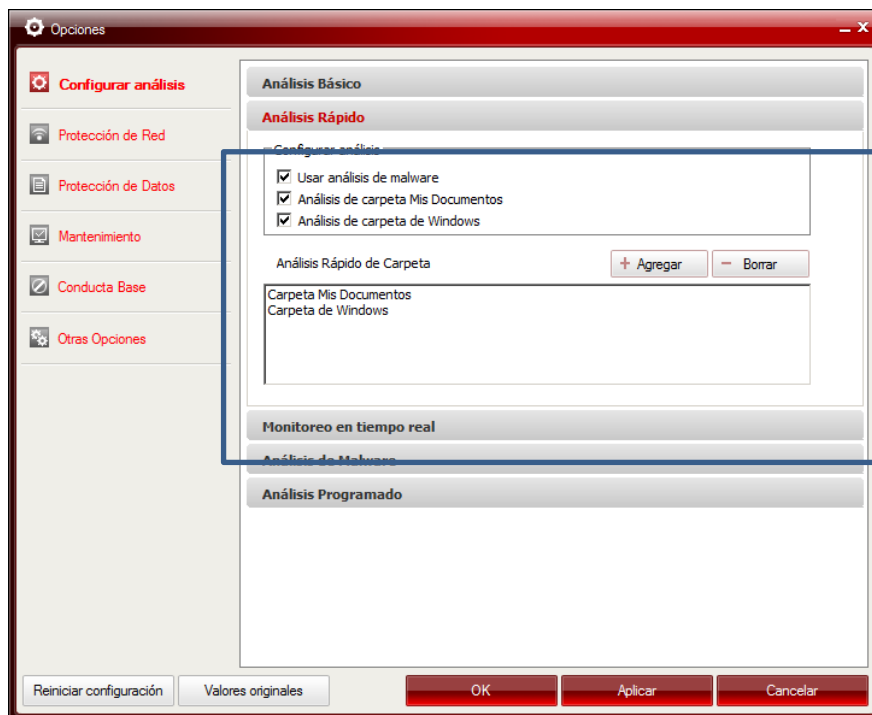
② Análisis Rápido

a) Configurar Análisis

- El usuario puede seleccionar las carpetas para su análisis. Las Opciones de Análisis Rápido aplican cuando se ejecuta el Análisis Rápido desde el Menú principal de VRIS. Análisis rápido también ejecuta un análisis de memoria, sector de arranque, análisis de procesos y un análisis de auto-infección de acuerdo a la configuración del Análisis Básico.

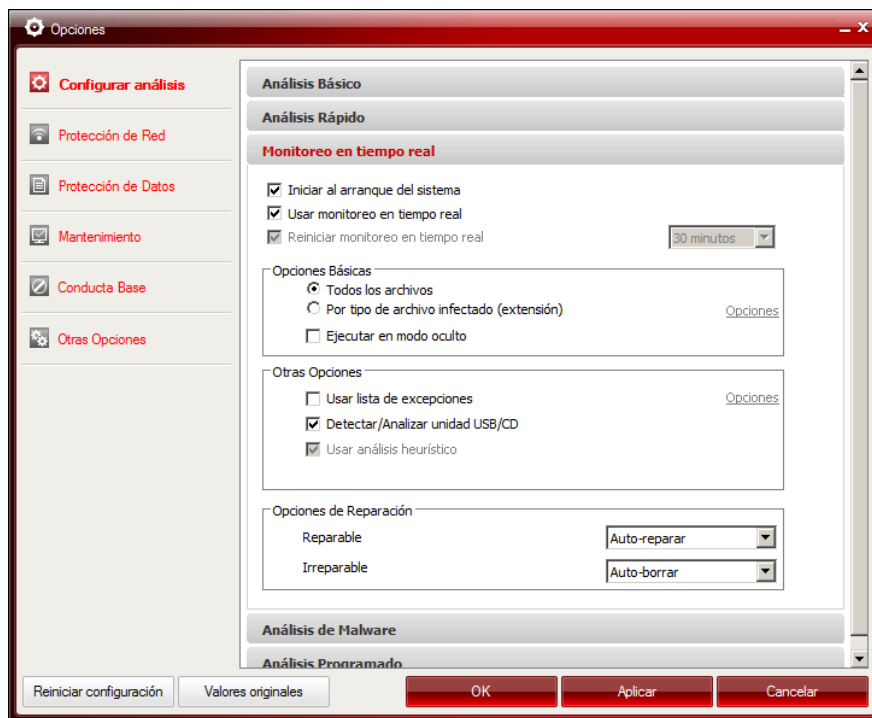
b) Análisis Rápido de Carpetas

- Las carpetas para análisis pueden ser especificadas usando la función Agregar o Borrar. Si el usuario agrega carpetas, usando la ventana de búsqueda, la ruta de la carpeta automáticamente se muestra su análisis rápido. El usuario no puede agregar archivos para análisis. Valores por defecto: Análisis de código malicioso, carpeta Mis Documentos, y la carpeta Windows).



[Fig. 2.56] Opciones de Análisis Rápido

③ Monitoreo en tiempo real



[Fig. 2.57] Opciones de Monitoreo en tiempo real

a) Iniciar al arranque del sistema

- En esta opción se habilita automáticamente el monitoreo en tiempo real al iniciar Windows. Si el monitoreo en tiempo real se inicia, se muestra una ventana de notificación.



[Fig. 2.58] Ventana de Estatus de Monitoreo en tiempo real

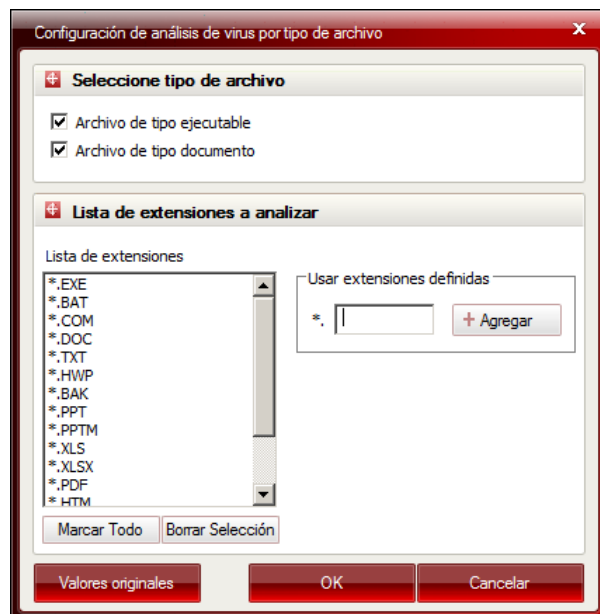
b) Usar monitoreo en tiempo real

- Activa la función del monitoreo en tiempo real que es el que realiza el monitoreo de archivos I/O. (Valor por defecto: Habilitado).

c) Opciones Básicas

- Todos los archivos: Escanea todos los tipos de archivos en tiempo real.
- Por tipo de archivo infectado (extensión): Esta opción analiza los archivos definiendo la extensión, las opciones disponibles son: Archivos ejecutables, documentos, y extensiones definidas por el usuario. Por defecto está activado el análisis de ejecutables y documentos. Las extensiones analizadas de documentos son las siguientes.

EXE	BAT	COM	DOC	TXT	HWP	BAK
PPTM	XLS	XLSX	PDF	HTM	MBD	XLK
PPT						



[Fig. 2.59] Configuración de Análisis de virus por tipo de archivo

- Ejecutar en modo oculto: Las detecciones de código malicioso y la acción requerida estarán en modo oculto. (Valor por defecto: Deshabilitado).

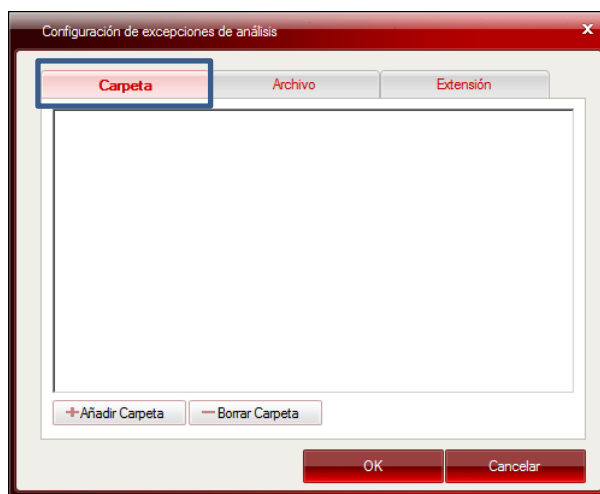


Referencia

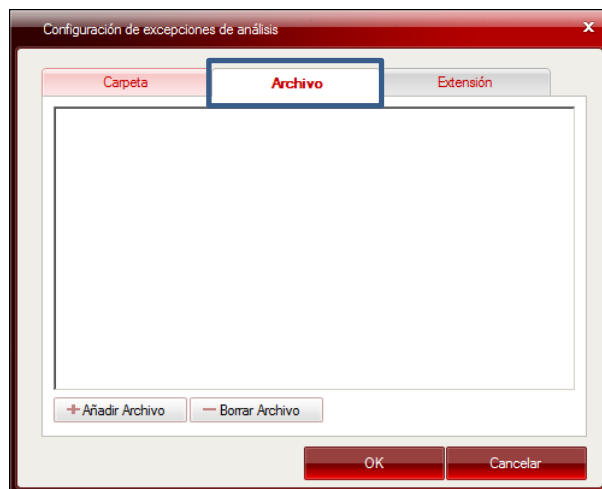
- ✖ Si el monitoreo en tiempo real está en modo oculto, la ventana de análisis no aparecerá.

d) Otras Opciones

- Usar lista de excepciones: Se puede configurar la lista de excepciones para el monitoreo. Se agregan carpetas y archivos a la exclusión, a través del Explorador de Windows. Cuando se agregan extensiones a la exclusión, se hace de manera manual. (No hay configuración por defecto para esta opción).



[Fig. 2.60] Lista de carpetas excluidas del monitoreo



[Fig. 2.61] Lista de archivos excluidos del monitoreo

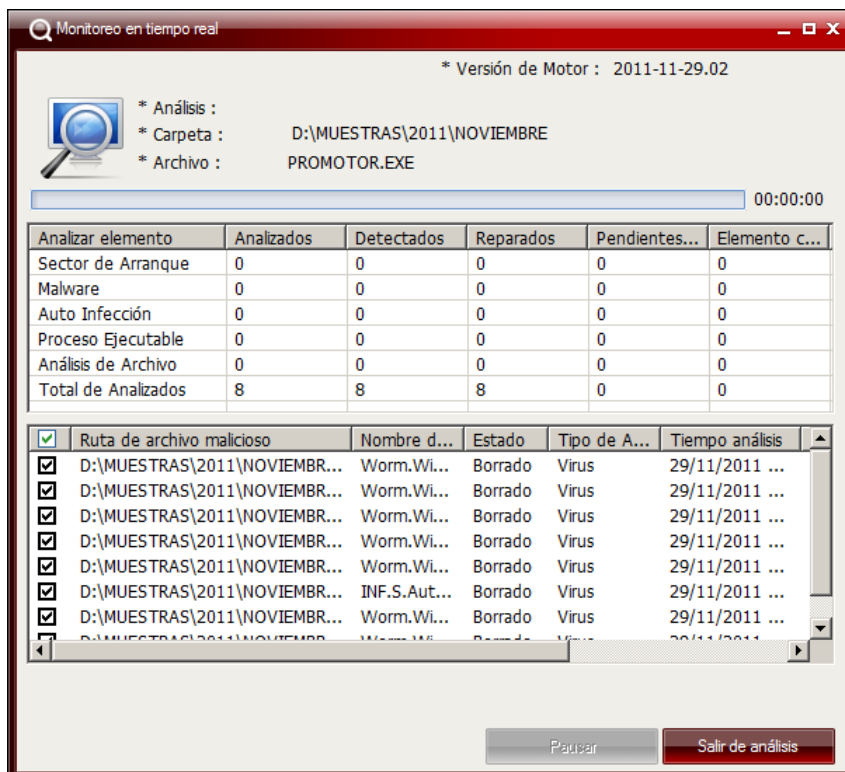


[Fig. 2.62] Lista de extensiones excluidas del monitoreo

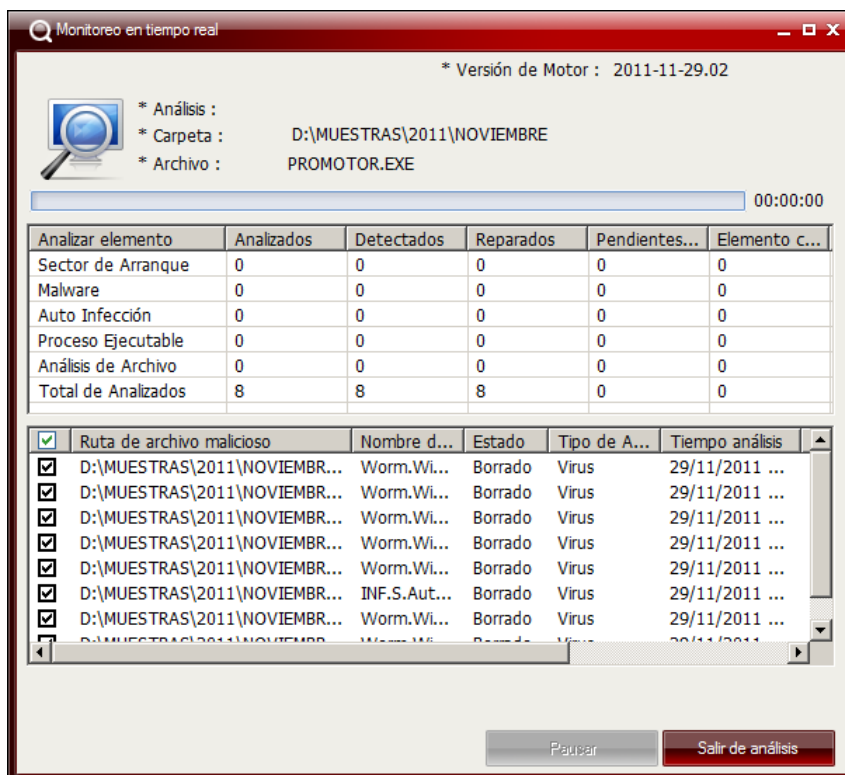
- Detectar/Analizar unidad USB/CD: Analiza las unidades extraíbles al ser detectadas por el sistema.
- Usar Análisis Heurístico: Analizar y detectar todos los archivos sospechosos para no perder ningún archivo malicioso.

e) Opciones de Reparación

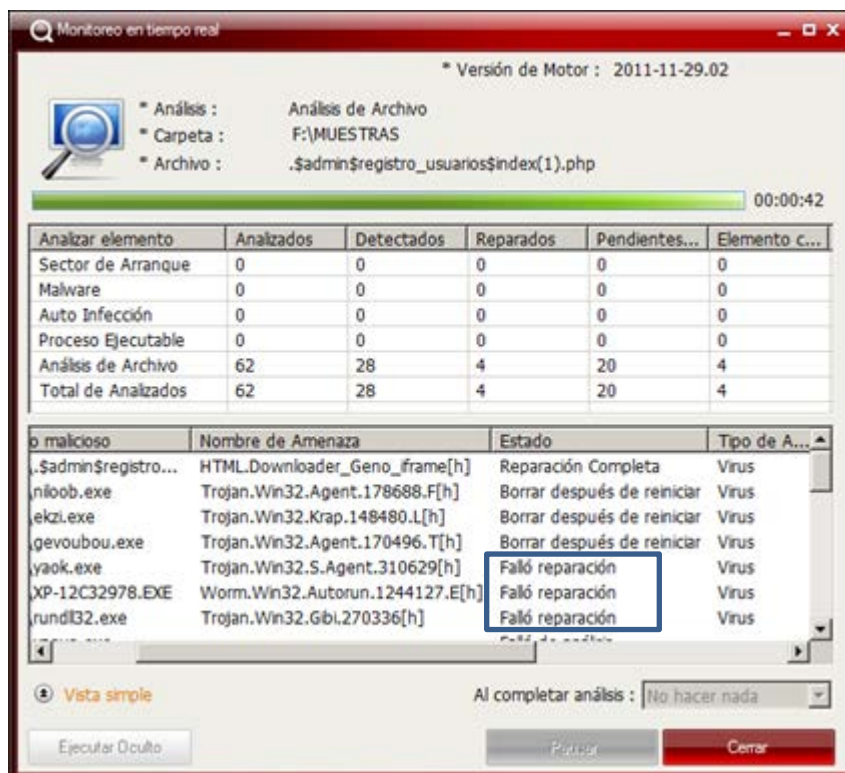
- Reparable: Si el código malicioso que es detectado se puede reparar, se actúa de acuerdo a la configuración, ya sea Ignorar, Auto-reparar o Auto-Borrar. (Valor por defecto: Reparar automáticamente).
- Irreparable: Si el código malicioso que es detectado no se puede reparar, se actúa de acuerdo a la configuración, ya sea Ignorar, Auto-reparar o Auto-Borrar. (Valor por defecto: Ignorar).



[Fig. 2.63] Ignorar, si la reparación en tiempo real es posible

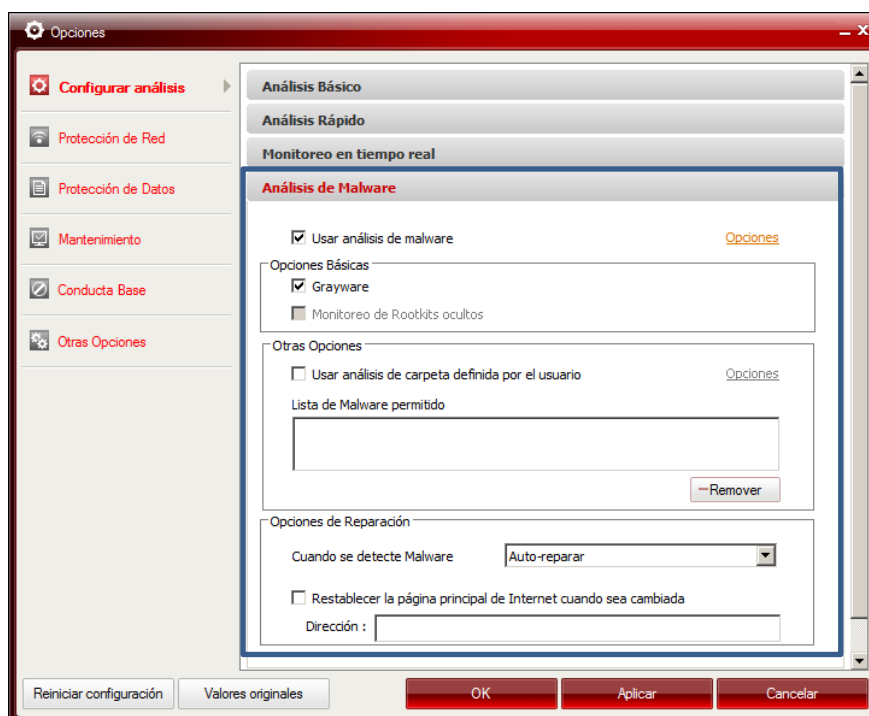


[Fig. 2.64] Auto-borrar, si la reparación en tiempo real es posible



[Fig. 2.65] Auto-borrar, si la reparación en tiempo real es posible

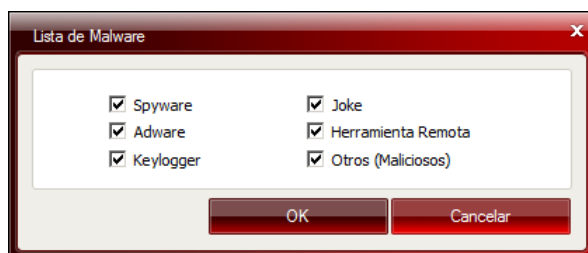
④ Análisis de Código Malicioso



[Fig. 2.66] Opciones de Análisis de Código Malicioso

a) Opciones Básicas

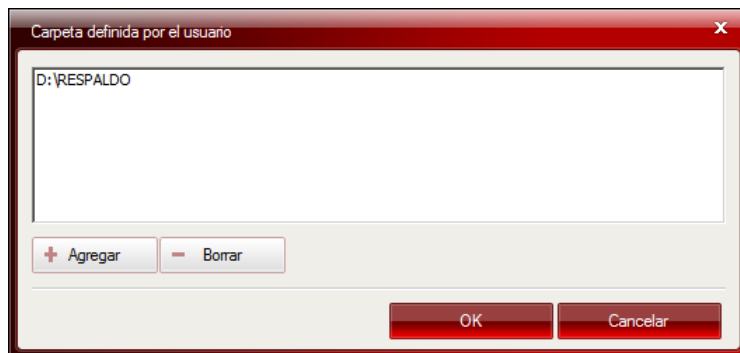
- Usar análisis de código malicioso: Incluye programas potencialmente dañinos en el análisis de código malicioso. Programas potencialmente dañinos son Spyware, Joke, Adware, Herramientas remotas, Keyloggers y otros (Programas Maliciosos). (Valor por defecto: Todo habilitado).
 - Spyware: Escanea infecciones por spyware.
 - Adware: Escanea infecciones por adware.
 - Key Loggers: Escanea infecciones de keyloggers.
 - Joke: Escanea infecciones por jokes.
 - Herramientas remotas: Escanea infecciones por herramientas remotas.
 - Otros (Programas Maliciosos): Escanea programas potencialmente dañinos, excepto los siguientes:
- Grayware: Escanea infecciones por grayware. En los valores por defecto se escanea grayware. (Habilitado).
- Monitoreo de Rootkits ocultos: Escanea los rootkits ocultos para prevenir el robo de información financiera.



[Fig. 2.67] Opciones de Lista Código Malicioso

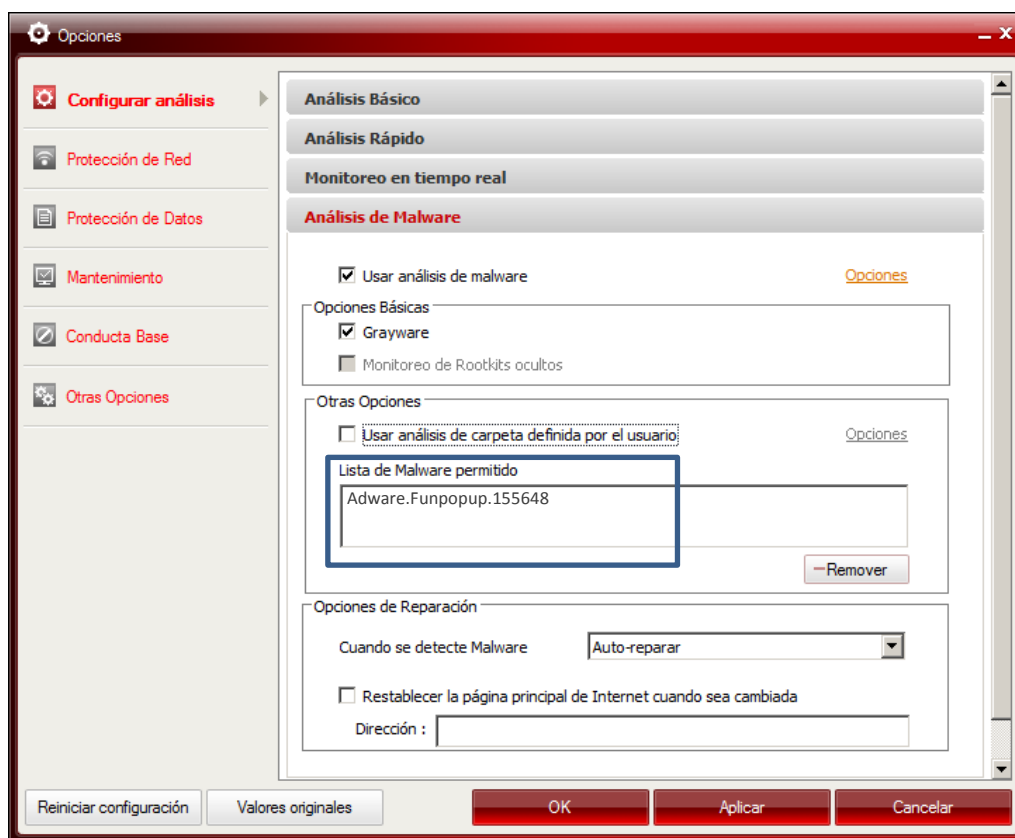
b) Otras opciones

- Usar análisis de carpeta definida por el usuario: Excluye carpetas del análisis de programas potencialmente dañinos. La lista de exclusiones es válida para el Análisis Personalizado, Análisis Rápido y Análisis Programado. (Valor por defecto: Deshabilitado).



[Fig. 2.68] Carpeta definida por el usuario

- Lista de Malware permitido: Esta opción registra los códigos maliciosos excluidos del análisis. (Valor por defecto: Ninguno).



[Fig. 2.69] Lista de Malware permitido

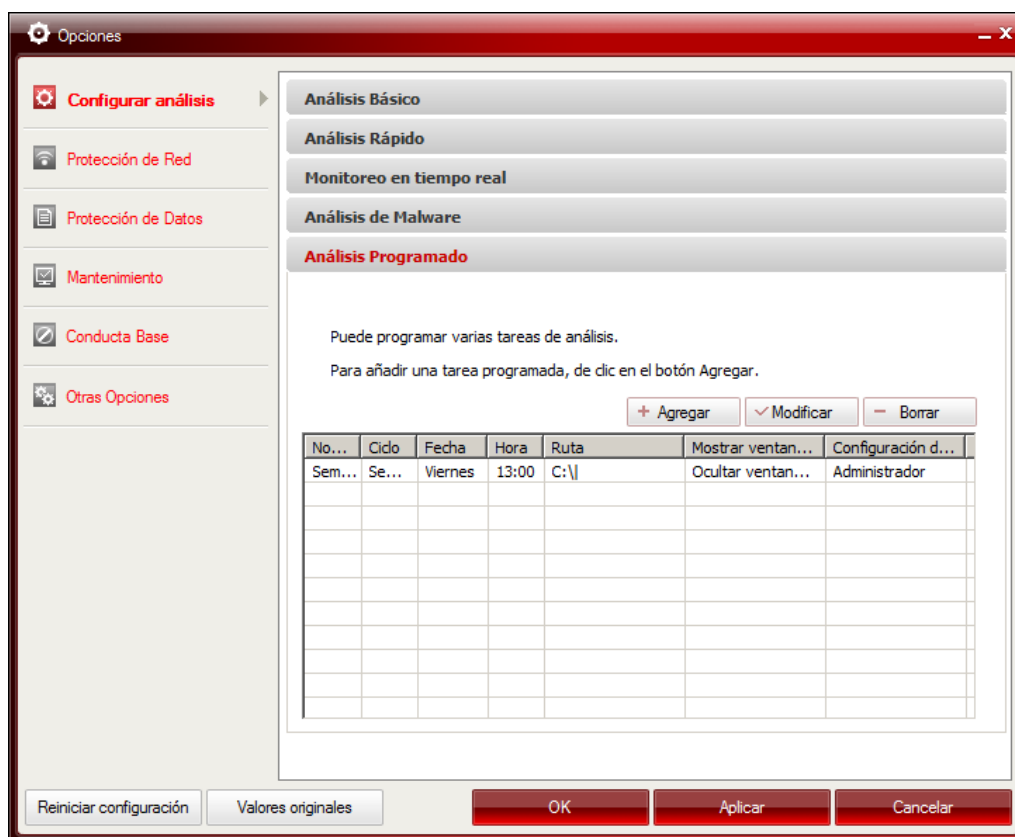
- Remove: Elimina los códigos permitidos en la lista.

c) Opciones de Reparación

- Cuando se detecte malware: Respuesta a la detección de códigos maliciosos en el sistema. El usuario puede seleccionar "Ignorar" o "Auto-reparar", cuando algún código es detectado. (Valor por defecto: Ignorar).

- Restablecer la página principal de Internet cuando sea cambiada: Es una opción para prevenir que código malicioso cambie la dirección de inicio del navegador. (Valor defecto: Ninguno).

⑤ Análisis programado

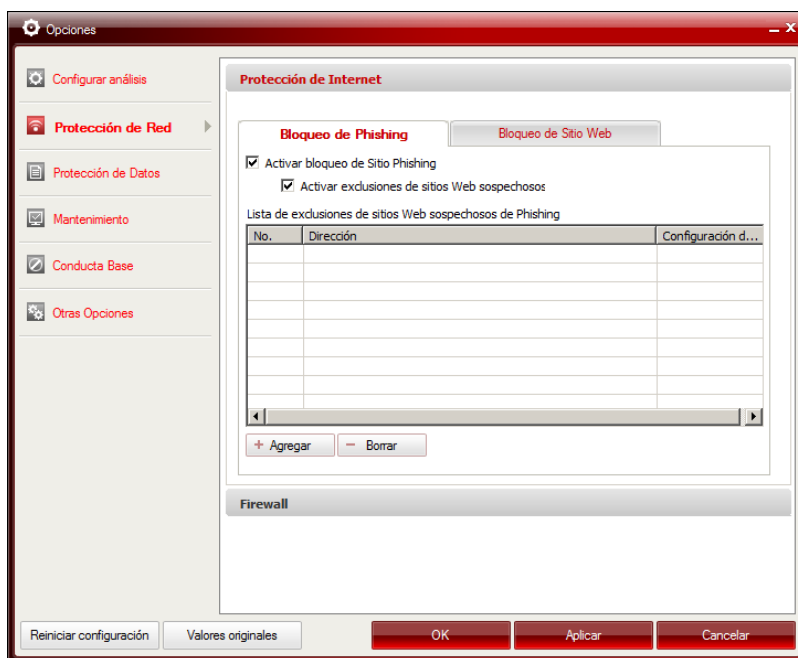


[Fig. 2.70] Opciones de Análisis Programado

- El usuario puede configurar el análisis de código malicioso en el horario que el desee. No existe ningún análisis por defecto.
- El análisis se puede programar diario, semanal o mensual. Aplicando la Opción “Aleatorio”, el análisis se hará en cualquier horario.
- Si se selecciona “Ejecutar en Modo Oculto”, el análisis no mostrará ninguna ventana .
- Se agregan carpetas al análisis desde el botón “Agregar”.
- Se finaliza la configuración del análisis dando clic en el botón “OK”.
- Seleccionando un análisis y dando clic en el botón “Modificar”, el análisis puede ser editado.
- Seleccionando un análisis y dando clic en el botón “Borrar”, el análisis puede ser eliminado. Si se da clic en el botón “Cancelar” la ventana de configuración será cerrada.
- El usuario puede generar diferentes análisis personalizados dando clic en el botón “Agregar”.
- Si genera un análisis igual a uno ya establecido el segundo análisis no se ejecutará.
- La información del análisis será registra como “Iniciado” y “Completado”, en el Visor de eventos.

2.5.2 Protección de Red

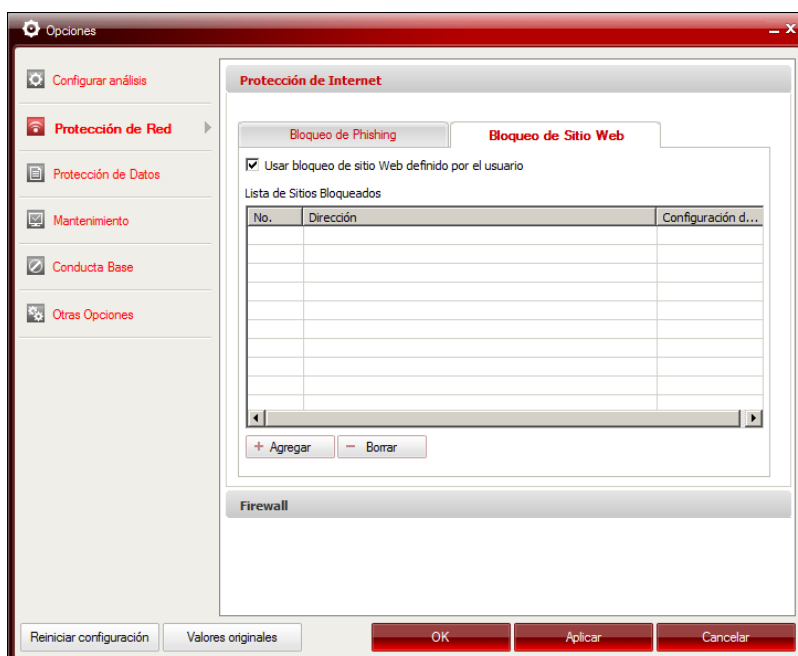
a) Bloqueo de Phishing



[Fig. 2.72] Opciones de Bloqueo de Phishing

- En esta configuración se puede Habilitar/Deshabilitar el bloqueo de sitios, y la configuración es aplicada vía política de VMS. Las exclusiones de sitios de phishing se muestran en la pantalla.

b) Bloqueo de sitios Web

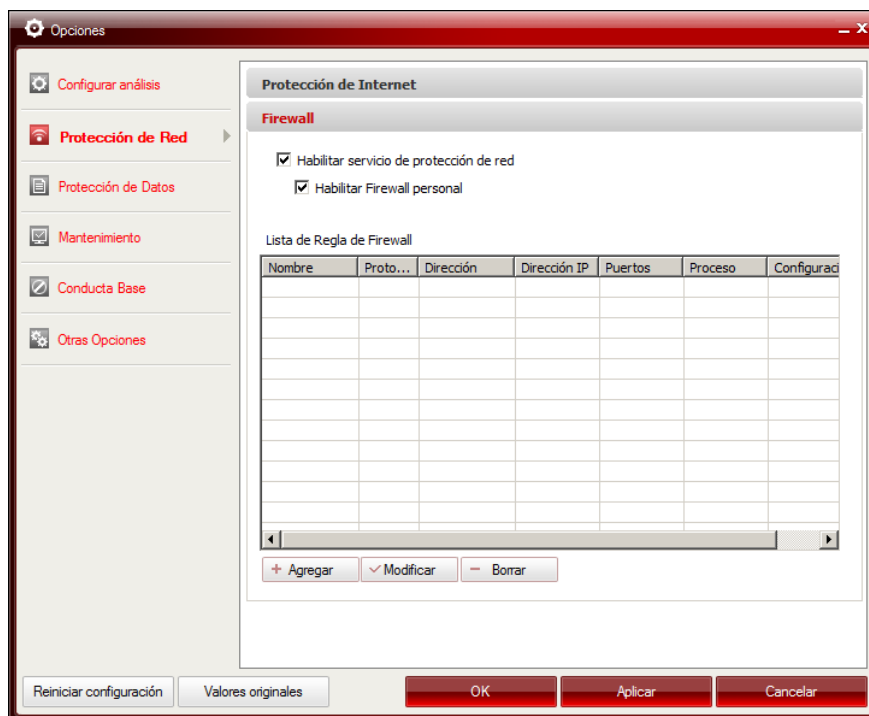


[Fig. 2.73] Opciones de Sitios Web

- La opción de Bloqueo de Sitios Web bloquea el acceso a los sitios específicos. Estos sitios pueden ser aplicados vía política de VMS. (Valor por defecto: Habilitado).

c) Firewall

➡ Configuración de Regla de Firewall



[Fig. 2.74] Configuración de Firewall

- El usuario puede permitir o bloquear el intercambio de datos con otras computadoras, ya sea vía internet o una red local. Esta configuración también puede realizar bloqueos de amenazas como el “hacking”, así la computadora está más protegida.
- Agregar: Para proteger la red local, agrega una regla de firewall.

➤ General

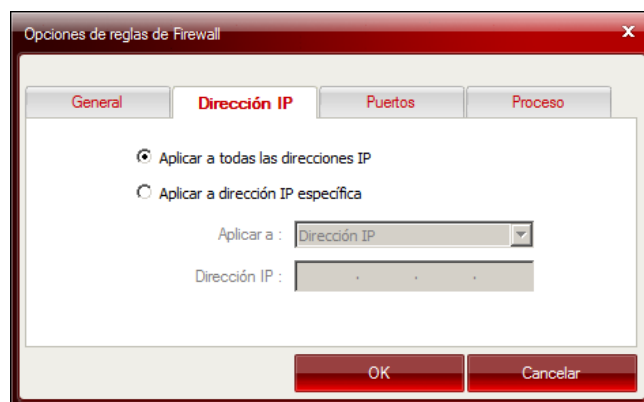
- Nombre de la regla de firewall: Se especifica el nombre de la regla.
- Protocolo: Se selecciona el protocolo de la regla de firewall, TCP y UDP pueden ser seleccionados. (Valor por defecto: Ninguno)
- Control de Red: Acción para aplicar a la regla de firewall. El usuario puede seleccionar entre: Permitir Todo, Permitir Salida, Permitir entrada, Bloquear Todo, Bloquear Salida y Bloquear Entrada.



[Fig. 2.75] Firewall – Pestaña General

➤ Dirección IP

- Aplicar a todas las direcciones de Red: La regla aplica para todas las direcciones IP.
- Aplicar a dirección IP específica: La regla aplica para dirección IP ingresada.



[Fig. 2.76] Firewall – Pestaña Dirección IP

➤ Puertos

- Aplicar a Todos: La regla aplica para todos los puertos de comunicación.
- Aplicar a un puerto: La regla aplica para el puerto de comunicación ingresado.



[Fig. 2.77] Firewall – Pestaña Puertos

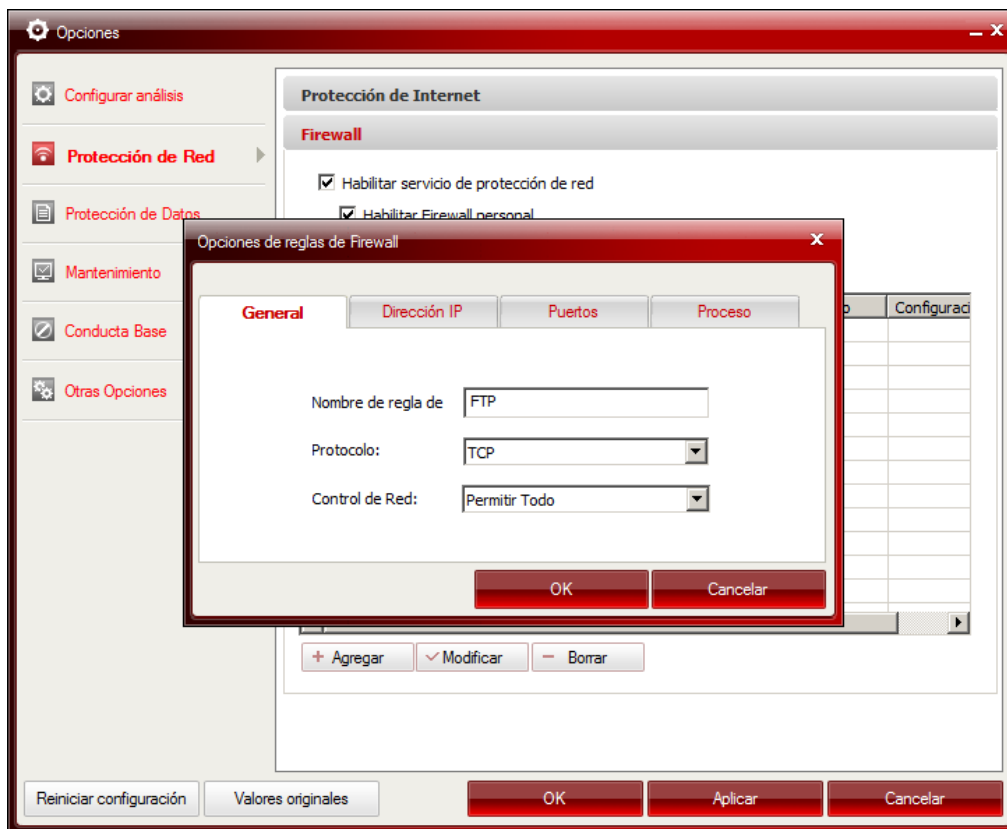
➤ Proceso

- Nombre de Proceso: La regla aplica para el proceso seleccionado.
- Ruta del Proceso: Se ingresa la carpeta donde se encuentra el proceso.



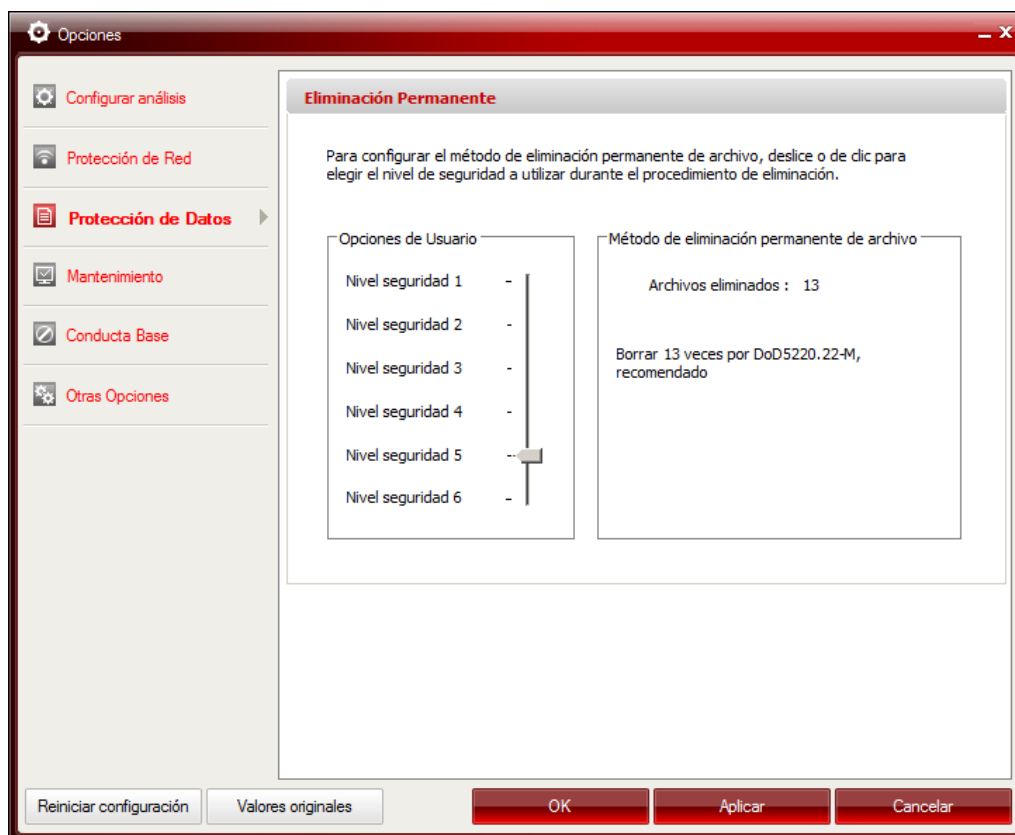
[Fig. 2.78] Firewall – Pestaña Proceso

- Ejemplo: Para generar una regla que permita el acceso a un FTP que se encuentre en el sistema donde está instalado VRIS, se debe generar una regla donde se permita el acceso.
- Modificar: Una regla de firewall puede ser editada, dando clic en la opción “Modificar”.
- Borrar: Se puede eliminar cualquier regla seleccionada.



[Fig. 2.79] Firewall – Pestaña Proceso

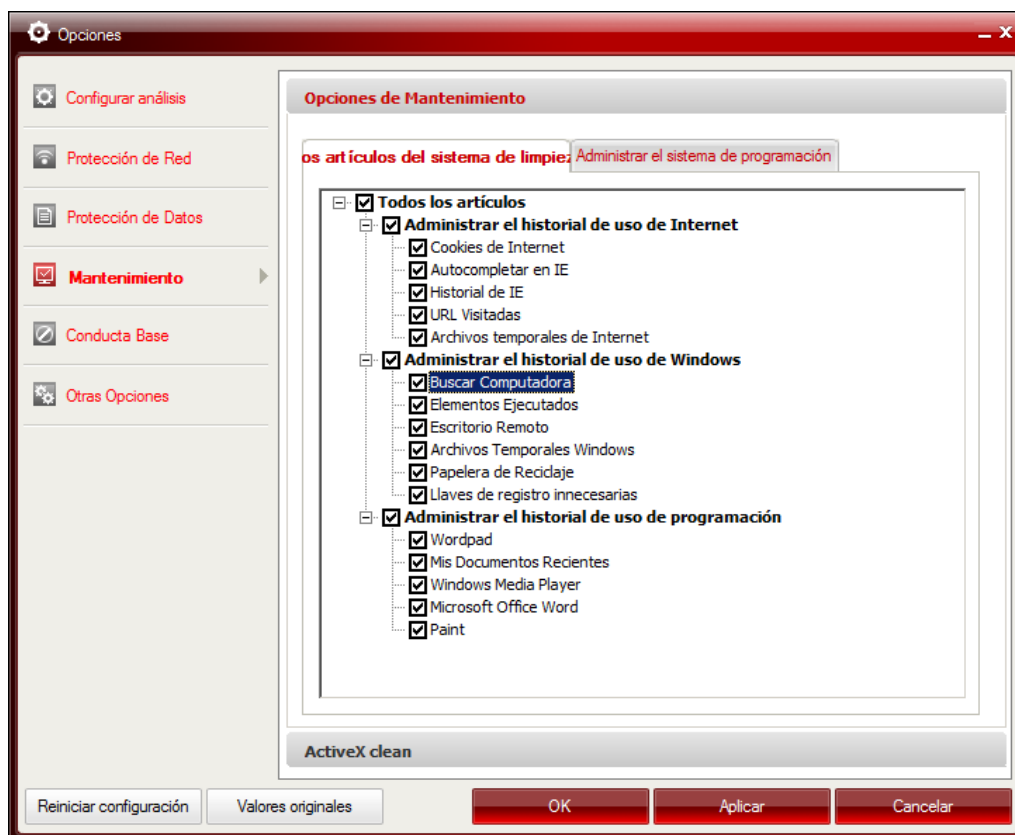
2.5.3 Protección de Datos



[Fig. 2.80] Selección del método de eliminación de archivos

- Cuando se eliminan archivos a través de la Protección de Datos, los archivos son eliminados de manera permanente de acuerdo al nivel seleccionado en la configuración. Para el método de eliminación permanente se puede seleccionar entre diferentes algoritmos de borrado.
- Básicamente, en los niveles 1 y 2 es imposible la recuperación de archivos. Entre el Nivel 3 y 6 el software y hardware no puede ser recuperado. (Valor por defecto: 5)

2.5.4 Mantenimiento



[Fig. 2.81] Opciones de Mantenimiento

- En las Opciones de Mantenimiento, este seguro de seleccionar las opciones siguientes.

➡ Administrar el historial del uso de Internet

- Cookies de Internet
- Autocompletar de IE
- Historial de IE
- URL Visitadas
- Archivos temporales de Internet

➡ Administrar el historial del uso de Windows

- Buscar Computadora
- Elementos Ejecutables
- Escritorio Remoto
- Archivos Temporales de Windows
- Papelera de Reciclaje
- Llaves de registro innecesarias

■➔ Administrar el historial del uso de Programación

- Wordpad
- Mis Documentos Recientes
- Windows Media Player
- Microsoft Office Word
- Paint

2.5.5 Otras Opciones



[Fig. 2.82] Opciones Complementarias

- Opciones como Auto-Defensa de Hauri, Easy Robot, Registro de eventos, Opciones avanzadas, Cuarentena y otras funciones pueden ser configuradas.

➡ Opciones de Auto Defensa de HAURI

- Se recomienda activar Auto Defensa de HAURI: Se puede activar la protección de archivos, de procesos, registros y la inyección de DLLs. Esta opción previene la alteración, modificación, terminado de los archivos y procesos críticos de VRIS. (Valor por defecto: Habilitado).
- Protección de Archivos: Monitorea los archivos de sistema registrados en el Sistema de Archivos (FAT, NTFS, etc.) para cada Sistema Operativo. Cualquier programa no autorizado que intente acceder archivos de Hauri, carpetas de VMS, agente de VMS, carpeta de instalación de VRIS, será monitoreado y se le denegará el acceso. Las acciones de protección de archivos son las siguientes. (Valor por defecto: Habilitado).

① Escritura (Creación, Edición), Los archivos y carpetas de VRIS y VRSP serán protegidos de acceso no autorizado.

② Si es un proceso que se encuentra en la lista de procesos permitidos, el resultado será "exitoso", por lo que podrá escribir o borrar en las carpetas de Hauri. Si es un procesos no autorizado no podrá realizar ninguna acción.

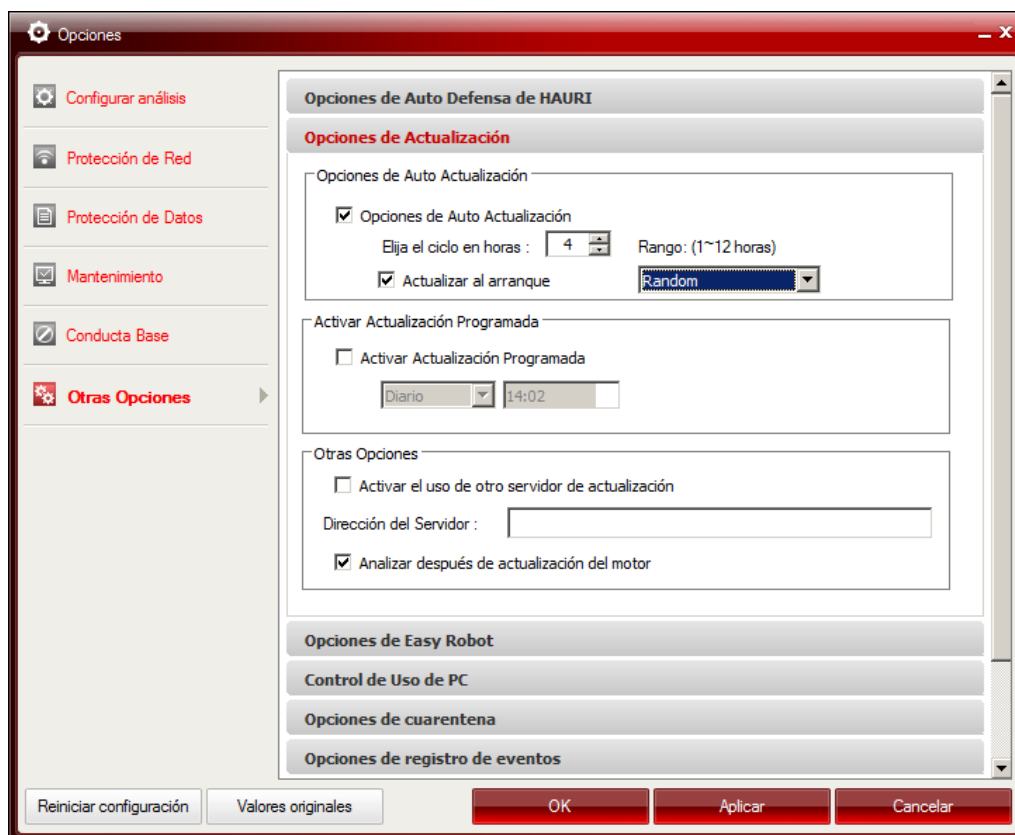
③ El controlador en tiempo real bloquea al malware de realizar cualquier acción sobre las carpetas de Hauri (c:\Archivos de Programa\Hauri).

- ▶ Protección de proceso: Bloquea/Permite la rutina de terminación de procesos a través de Win32Api del Sistema a nivel kernel con enlace SSDT. Los objetivos para la prevención del terminado de procesos está dividido en procesos y subprocesos. (Valor por defecto: Activado).
- ▶ Protección de registro: Después de conectar con el sistema SSDT, se monitorea el registro de los productos de Hauri. La protección del registro sirve para analizar si el procesos que pide la tarea de obtener el nombre del proceso es de los productos Hauri. (Valor por defecto: Activado).
- ▶ Protección de inyección de DLLs.

■➡ Opciones de Actualización

① Opciones de Auto Actualización

- Después de ejecutar la actualización, vaya a la configuración.
- Después de acceder a la configuración, habilite la opción de auto actualización.
- Si se habilita la auto actualización, esta se ejecutara automáticamente para realizar la actualización desde los servidores de Hauri. (Valor por defecto: 4hrs).



[Fig. 2.83] Opciones de Actualización

- Se puede configurar el servidor de actualizaciones del cual se realizara la descarga.
 - El valor máximo para ingresar la dirección web es de 260 caracteres.
 - Activar el uso de otro servidor de actualización: El usuario puede especificar otra dirección de servidor de actualización.
- ※ Como los ambientes de trabajo pueden variar, debe contactar a Hauri la para la configuración del servidor.

➡ Easy Robot

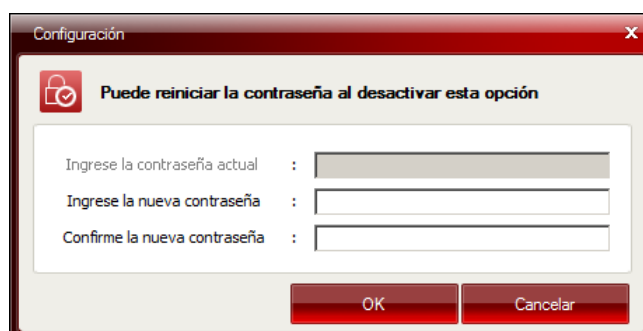
- **Análisis Rápido:** El usuario puede activar esta opción para que al momento de ejecutar el Análisis desde el Menú Principal. El Análisis Rápido se ejecuta con su configuración preestablecida.
- **Mantenimiento:** El usuario puede activar esta opción para que al momento de ejecutar el Análisis desde el Menú Principal. El Mantenimiento se ejecuta con su configuración preestablecida.



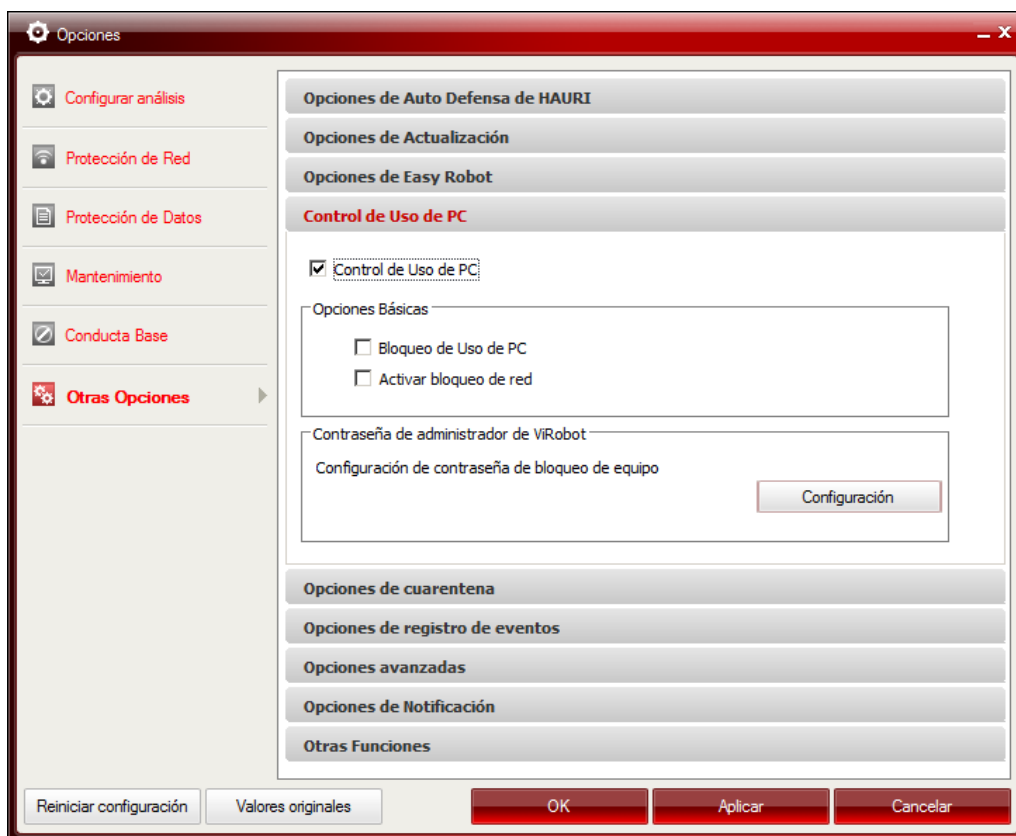
[Fig. 2.84] Opciones de Easy Robot

➡ Control de Uso de PC

- El bloqueo del Uso del PC: Esta opción bloquea el sistema y previene que usuarios utilicen el equipo. (Valor por defecto: Desactivado).
- Bloqueo de Uso de Red: Bloquea la comunicación en la red mientras este se encuentre funcionando. (Valor por defecto: Desactivado).
- Contraseña de Administrador de ViRobot: Si el sistema es bloqueado, será necesario ingresar la contraseña para su desbloqueo. (Valor por defecto: Desactivado).



[Fig. 2.85] Configuración de contraseña de Control de Uso de PC



[Fig. 2.86] Configuración de Control de Uso de PC



[Fig. 2.87] Pantalla de Restricción de Control de Uso de PC

➡ Opciones de Cuarentena

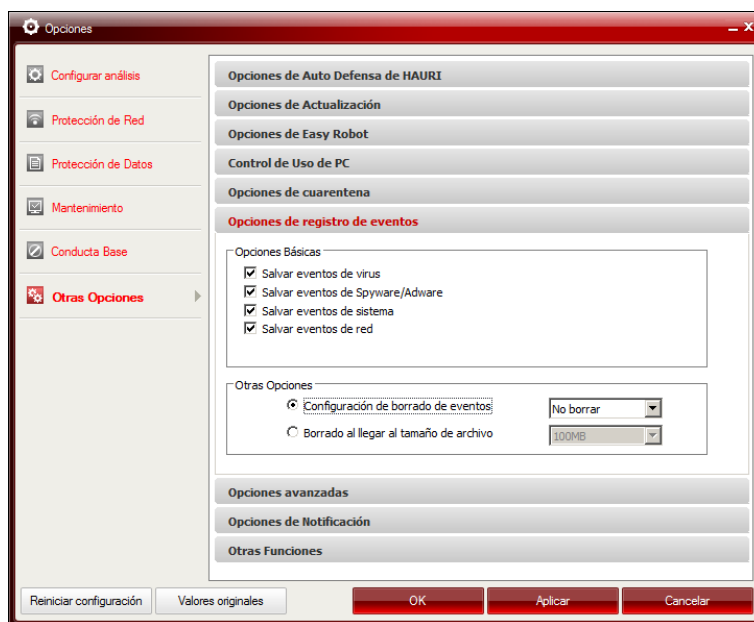
- Respaldar antes de reparar (excepto archivos comprimidos): Cuando se repara o elimina el malware detectado, estos archivos son guardados en la cuarentena (Valor por defecto: Habilitado).
- Si se excede la capacidad, enviar a cuarentena después de borrar información existente: Cuando el número de elementos excede el límite, se empiezan a eliminar los datos existentes. (Valor por defecto: Habilitado).
- Límites de Respaldo/Cuarentena: Cantidad de elementos a guardar en la cuarentena. (Rango: desde 1,000 hasta 10,000 elementos).



[Fig. 2.88] Opciones de Cuarentena

➡ Opciones de registro de eventos

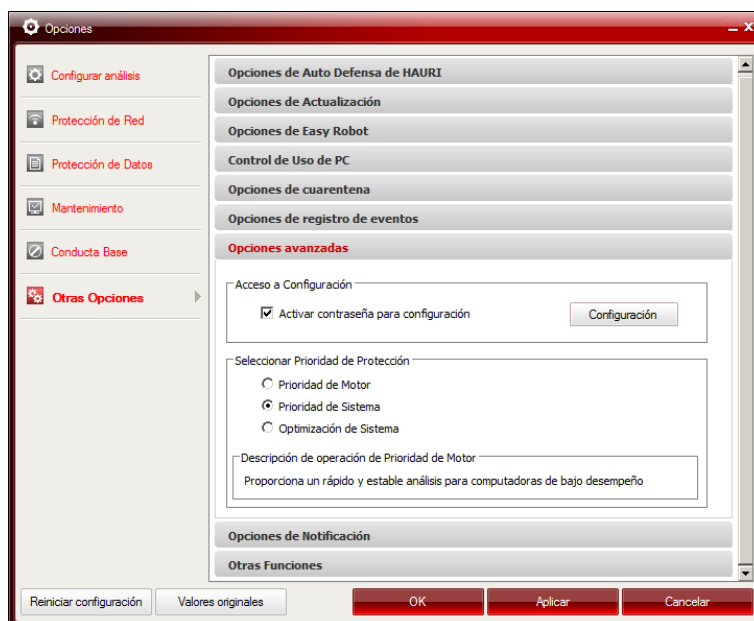
- Salvar elementos de virus: El historial de detección de malware es guardado. (Valor por defecto: Habilitado).
- Salvar eventos de Spyware/Adware: El historial de detección de programas potencialmente dañinos es guardado. (Valor por defecto: Habilitado).
- Salvar elementos de sistema: Acciones de los módulos de VRIS son guardados. (Valor por defecto: Habilitado).
- Configuración de borrado de eventos: Se puede seleccionar entre las opciones, 1 día y 15 días o No borrar. (Valor por defecto: No borrar).
- Borrado al llegar al tamaño de archivo: Cuando el tamaño del log excede, ya sea, 4MB, 10MB, 50MB, o 100MB, según allá sido configurado.



[Fig. 2.89] Opciones de Registro de Eventos

➡ Opciones Avanzadas

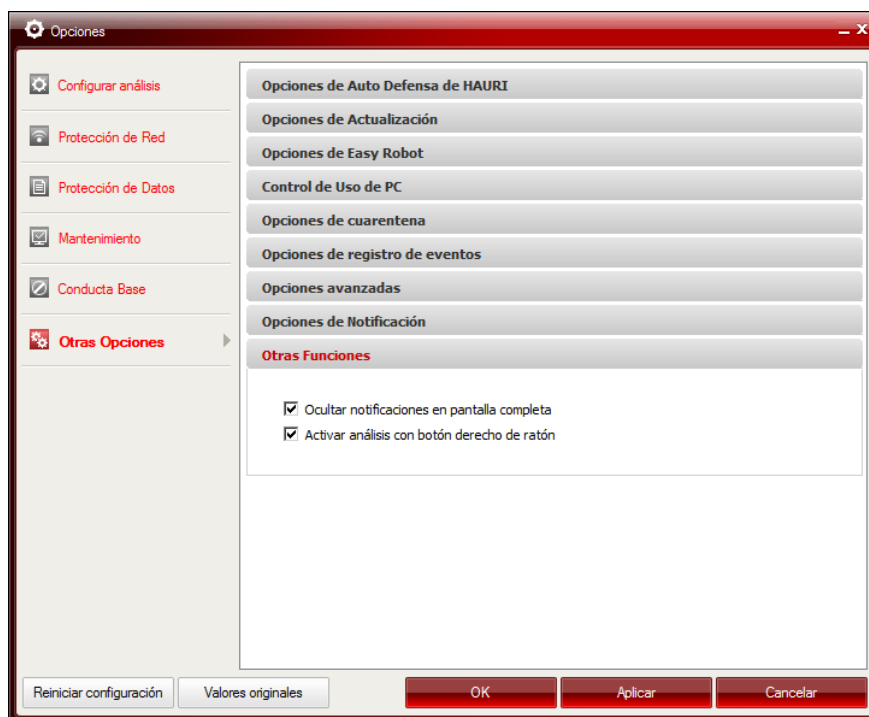
- Acceso a Configuración: Se activa una contraseña para proteger la configuración de VRIS.
- Seleccionar prioridad de protección: Selecciona el motor de análisis de malware. Si se selecciona Prioridad de Motor, se combina el motor de Bitdefender y Hauri. Si se selecciona Prioridad de Sistema, solo se activa el motor de Hauri. Si se activa Optimización de Sistema, VRIS realiza un análisis de desempeño del equipo y aplica la configuración recomendada.



[Fig. 2.90] Opciones Avanzadas

➡ Otras Funciones

- Ocultar notificaciones en pantalla completa: Si alguna aplicación está siendo ejecutada en pantalla completa, los mensajes de notificación de VRIS son ocultos. (Valor por defecto: Desactivado).
- Activar análisis con botón derecho del mouse: Al seleccionar algún archivo o carpeta, VRIS agrega la función de análisis en el menú contextual que aparece al dar clic en el botón derecho del mouse. (Valor por defecto: Activado).



[Fig. 2.91] Otras Funciones

2.6 Actualización

Esta función de VRIS ejecuta la actualización del motor y firmas para detección de malware.

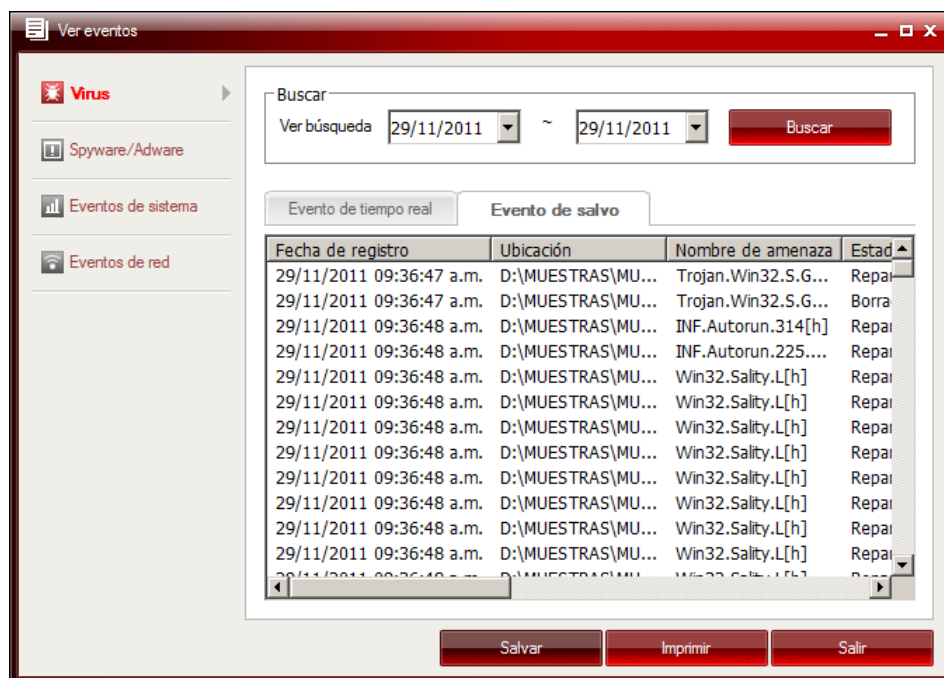


[Fig. 2.92] Opciones Avanzadas

- Accediendo al SUS, Servidor de Actualización de Firmas (Signature Update Server por sus siglas en ingles), que se establece en la configuración de actualización, se descarga la última versión del motor, las firmas y módulos de VRIS.
- Si la tarjeta de red no funciona correctamente, o el puerto 80 está bloqueado en la configuración de la red, la actualización no puede ser llevada a cabo y aparecerá el mensaje “Falla de Actualización”.
- Si la versión actual del motor y las firmas es igual a la existente en el servidor de actualización, VRIS no se actualizara y le notificara al usuario que se cuenta con las versiones más recientes.
- Si la red es desconectada mientras se realiza la actualización, aparecerá un mensaje de error.
- Una vez finalizada la descarga de archivo, se analizan procesos infectados por malware al activar la opción “Escanear después de actualizar”, y se repararan los archivos infectados.
- Después de la actualización se realiza un análisis con la configuración siguiente.
 - ① Se realiza un análisis de memoria
 - ② Se reparan automáticamente archivos infectados por malware.
 - ③ Aunque no se ejecute un análisis de infección en el registro y/o alteración de página de inicio del navegador por algún programa potencialmente dañino, si se analizan los códigos maliciosos a través del motor antivirus.
- Los eventos de la actualización al inicio, la finalización y elementos se muestran en el visor de eventos.

2.7 Visor de eventos

El visor de eventos nos muestra los registros de detección de malware, spyware, operación, errores y registros de la cuarentena. El registro se divide en dos, eventos en tiempo real que nos muestra los eventos actuales y eventos salvados que nos muestra la información de los eventos guardados. Estos eventos pueden ser exportados a Excel, para después poder ser impresos.



[Fig. 2.93] Visor de eventos

① Eventos de virus

- Todos los eventos de virus que han sido detectados por VRIS son guardados. Se muestra la siguiente información de los eventos.
 - a) Fecha de registro: Se muestra la fecha y hora de la detección con la nomenclatura año-mes-día hora-minuto-segundo.
 - b) Ubicación: Se muestra la ruta completa y el nombre del archivo detectado.
 - c) Nombre de la amenaza: Se muestra el nombre de la firma.
 - d) Estado: Se muestra el estatus de la detección, Reparación exitosa/Borrado/Reparable.
 - e) Tipo de amenaza: Se muestra el tipo de infección.
 - f) Tipo de Análisis: Se muestra la información del análisis con el cual fue detectado el archivo.
 - g) Cuenta de usuario: Se muestra la información de la cuenta con la cual fue detectada la amenaza.
 - h) Nombre de la computadora: Se muestra el nombre de la computadora del sistema actual.

② Eventos de Spyware/Adware

- Todos los eventos de Spyware/Adware que han sido detectados por VRIS son guardados. Se muestra la siguiente información de los eventos.
- a) Fecha de registro: Se muestra la fecha y hora de la detección con la nomenclatura año-mes-día hora-minuto-segundo.
- b) Ubicación: Se muestra la ruta completa y el nombre del archivo detectado.
- c) Nombre de la amenaza: Se muestra el nombre de la firma.
- d) Estado: Se muestra el estatus de la detección, Reparación exitosa/Borrado/Reparable.
- e) Tipo de amenaza: Se muestra el tipo de infección.
- f) Tipo de Análisis: Se muestra la información del análisis con el cual fue detectado el archivo.
- g) Cuenta de usuario: Se muestra la información de la cuenta con la cual fue detectada la amenaza.
- h) Nombre de la computadora: Se muestra el nombre de la computadora del sistema actual.

③ Eventos Sistema

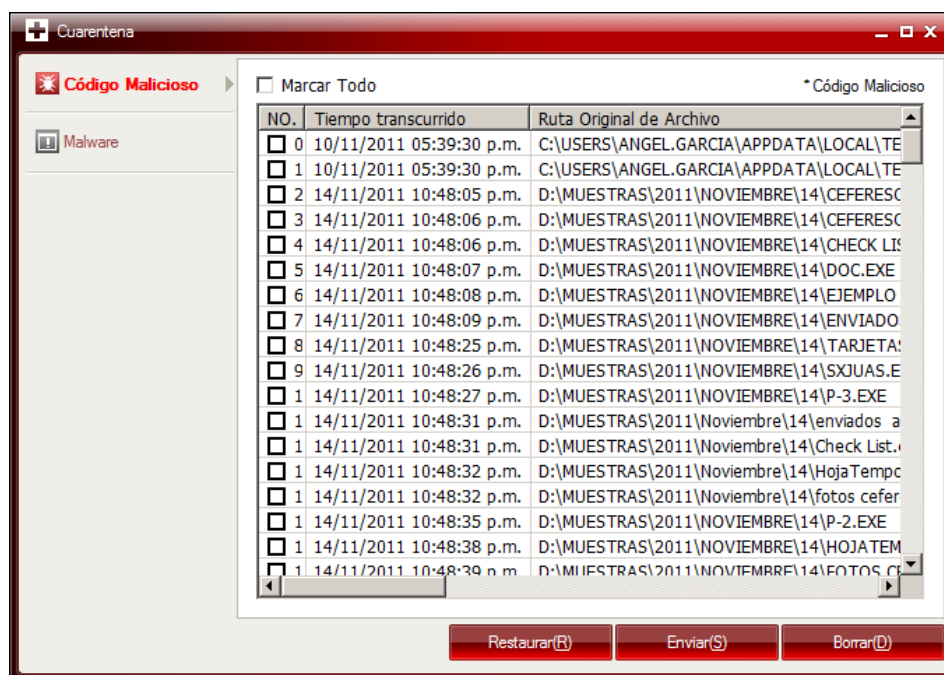
- Todos las acciones de los módulos de VRIS son guardados. Se muestra la siguiente información de los eventos.
- a) Fecha de registro: Se muestra la fecha y hora de la detección con la nomenclatura año-mes-día hora-minuto-segundo.
- b) Modulo en ejecución: Se muestra el modulo ejecutado.
- c) Estado: Muestra la información detallada del evento.
- d) Cuenta de usuario: Se muestra la información de la cuenta con la cual fue detectada la amenaza.
- e) Nombre de la computadora: Se muestra el nombre de la computadora del sistema actual.

2.8 Cuarentena



[Fig. 2.94] Cuarentena

- Si se repara o elimina algún malware, este es respaldado en la cuarentena, de acuerdo a la configuración.
- La cuarentena separa el almacenamiento de malware y código malicioso, los archivos almacenados pueden ser restaurados.



[Fig. 2.95] Cuarentena

① Código malicioso

➤ Las columnas se muestran de la siguiente manera.

- a) No.: Se muestra el orden de los elementos de la cuarentena, los elementos están en orden descendente, desde 0 hasta el final.
- b) Tiempo transcurrido: Se muestra la fecha en que el elemento fue creado en la cuarentena.
- c) Ruta original del archivo: Se muestra la ruta original del archivo cuando el elemento en la cuarentena fue creado.
- d) Tamaño original del archivo: Se muestra el tamaño original del archivo en bytes.
- e) Nombre de la amenaza: Se muestra el nombre de la firma.
- f) Versión del motor: Se muestra la información de la versión del motor que detectó la amenaza.
- g) Causa: Se muestra la tarea realizada y por que fue creado el elemento en la cuarentena.
- h) Clase de Actividad: Se muestra el análisis con el cual fue detectado.
- i) Usuario: Se muestra la cuenta de usuario activa al momento de la detección.

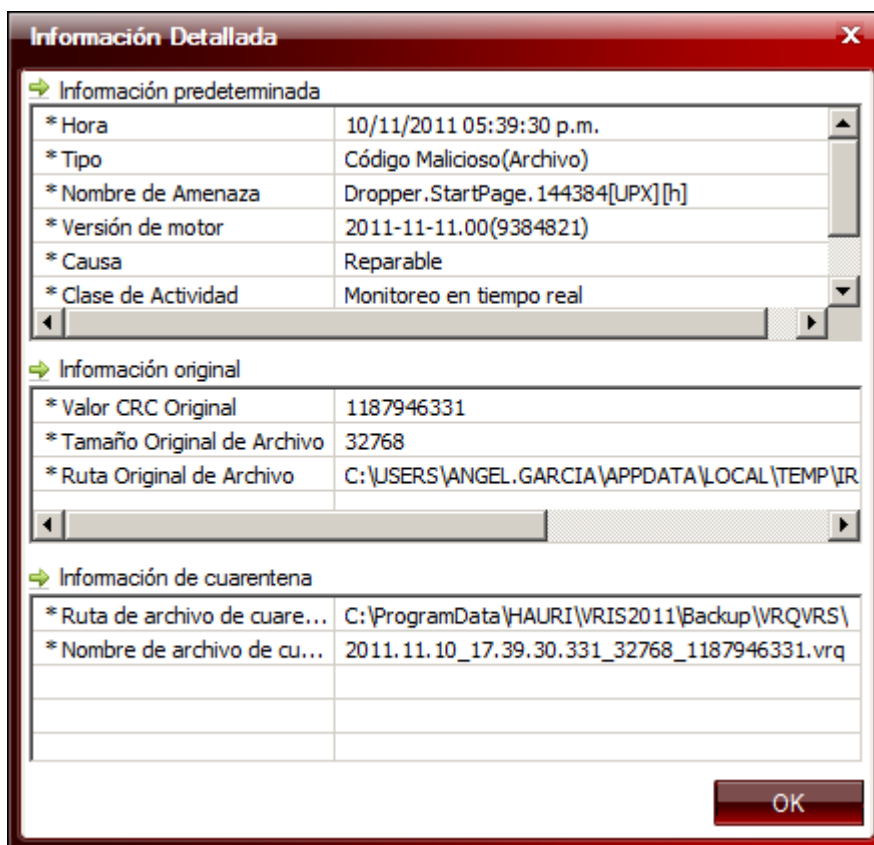
② Malware

➤ Las columnas se muestran de la siguiente manera.

- a) No.: Se muestra el orden de los elementos de la cuarentena, los elementos están en orden descendente, desde 0 hasta el final.
- b) Tiempo transcurrido: Se muestra la fecha en que el elemento fue creado en la cuarentena.
- c) Ruta original del archivo: Se muestra la ruta original del archivo cuando el elemento en la cuarentena fue creado.
- d) Tamaño original del archivo: Se muestra el tamaño original del archivo en bytes.
- e) Nombre de la amenaza: Se muestra el nombre de la firma.
- f) Versión del motor: Se muestra la información de la versión del motor que detectó la amenaza.
- g) Causa: Se muestra la tarea realizada y por que fue creado el elemento en la cuarentena.
- h) Clase de Actividad: Se muestra el análisis con el cual fue detectado.
- i) Usuario: Se muestra la cuenta de usuario activa al momento de la detección.

➡ Información

- El usuario quiere visualizar la información del archivo seleccionado.



[Fig. 2.96] Ventana de información de Malware

➡ Restaurar

- Recuperar a la carpeta original: Esta opción restaura el archivo a la carpeta original en la cual se encontraba al momento de la detección.
- Recuperar a otra carpeta: Esta opción restaura el archivo a la carpeta definida por el usuario.

➡ Enviar

- Si existe algún malware que no se pueda reparar, este es enviado a Hauri. Utilizando esta opción el archivo es enviado al Centro de Repuestas de Hauri. Al recibirse esta muestra se actualizará la reparación lógica del archivo.

➡ Borrar

- El archivo es eliminado de la cuarentena. Los archivos eliminados no pueden ser recuperados.